GOVERNMENT–INDUSTRY SYSTEM SAFETY CONFERENCE

Sponsored by the

NASA SAFETY OFFICE

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Washington, D. C.

MAY 26-28, 1971

at the

Goddard Space Flight Center,

Greenbelt, Maryland

25961

PROGRAM

CHAIRMAN: Philip H. Bolger
Assistant NASA Director of Safety

EXECUTIVE SECRETARY: Paul D. Davis
NASA Safety Office

Wednesday, May 26

Opening Remarks
Mr. Jerome F. Lederer
NASA Director of Safety

Welcome
Dr. John F. Clark, Director
Goddard Space Flight Center

Keynote Address
Honorable Jerry L. Pettis
U.S. Representative (California)

Perspective for System Safety
Honorable Willard J. Smith
Asst. Secretary for Safety and Consumer Affairs
Department of Transportation

SESSION I - New Developments in Safety

Session Chairman: Mr. Philip H. Bolger
Assistant NASA Director of Safety

Opening Remarks by Session Chairman

62 Communication of Risk
Dr. Raymond M. Wilmotte
Safety Consultant

63 System Safety Management - A New Discipline
Mr. W. C. Pope, Chief
Division of Safety Management
Department of Interior

64 Data Requirements Analysis in Support of System Safety
Mr. I. Irving Pinkel
Chief, Information Services and Publication Branch
Aerospace Safety Research and Data Institute
NASA - Lewis Research Center

65 Reflections on System Safety and the Law
Mr. Daniel F. Hayes, Sr.
Assistant NASA Director of Safety

Session I Question and Answer Period

SESSION II - System Safety in Aviation

Session Chairman: Mr. H. Kurt Strass, Director
Safety & Operating Systems Office
NASA Headquarters

Opening Remarks by Session Chairman

66 Why System Safety Programs Can Fail
Mr. Willie Hammer
Member, Senior Technical Staff
Hughes Aircraft Company

67 The Practical Application of Mishap Data in Army Aircraft System Safety Programs
LTC James T. Darrah, Jr.
U.S. Army Board of Aviation Accident Research

68 Some Thoughts about Systems Safety Assessment and Its Current Application in Aerospace
Mr. Peter R. Allison
Design Surveyor - Systems Coordination
British Air Registration Board

Pilot Safety for the X-24A Lifting Body Vehicle
Mr. John Cochrane
Senior Field Engineer
Martin Marietta Corporation

Session II Question and Answer Period

Thursday, May 27

SESSION III - System Safety Education

Session Chairman: Mr. Vernon L. Grose, Vice President
Tustin Institute of Technology

Opening Remarks by Session Chairman

System Safety Education Focused on Flight Safety
Mr. Eugene Holt
University of Southern California

System Safety Education Focused on Industrial Engineering
Dr. W. L. Johnston
Texas A&M University

System Safety Education Focused on System Management
Mr. Vernon L. Grose
George Washington University

Session III Question and Answer Period

SESSION IV - Requirements and Management

Session Chairman: Mr. Chuck McGuire
NASA Safety Office

Opening Remarks by Session Chairman

Contracting for System Safety
Dr. Leslie W. Ball
Director of Safety
NASA-Marshall Space Flight Center

Requirements for Systems Safety Programs as Delineated by MIL-STD-882
Mr. C. O. Miller, Director
Bureau of Aviation Safety
National Transportation Safety Board

Integrating System Safety into the Basic Systems Engineering Process
Mr. John W. Griswold
Reliability & System Safety Manager
Aerospace Group - The Boeing Company

Session IV Question and Answer Period

SESSION V - System Safety in Space Program

Session Chairman: Mr. W. J. Quinlivan
Manager, Flight Safety
Lockheed - California

Opening Remarks by Session Chairman

The Viking Project Safety Program
Mr. Donald H. Ward
Project Viking Safety Officer
NASA-Langley Research Center

System Safety in the Operational Phase
Mr. John Gera, Jr.
Manager, Division Safety
North American Rockwell

Lunar Module Program System Safety
Mr. William E. Scarborough
LM Safety Manager
Grumman Aerospace Engineering Corp.

System Safety in Manned vs. Unmanned Programs
Mr. George B. Mumma
Systems Safety Manager
Martin Marietta - Denver

The Reduction of a "Safety Catastrophic" Potential Hazard - A Case History
Mr. Joseph P. Jones
Staff Engineer, System Safety
Bendix Aerospace Systems Division

Session V Question and Answer Period

Friday, May 28

SESSION VI - System Safety, The Consumer, and General Industry

Session Chairman: Dr. Leslie W. Ball
Director of Safety
NASA-Marshall Space Flight Center

Opening Remarks by Session Chairman

Fault Tree Applications within the Safety Program of Idaho Nuclear Corporation
Dr. W. E. Vesely
Senior Technical Specialist
Computer Science Branch
Idaho Nuclear Corporation

Consumer Product Safety - A Systems Problem
Dr. Carl C. Clark
Staff Consultant on Product Safety
National Bureau of Standards

Application of System Safety to Rail Transit Systems
Mr. Thomas DeW. Styles
Chief, Railroad Safety Division
National Transportation Safety Board

Designing for Auto Safety
Mr. Elwood T. Driver
Director, Office of Operating Systems
Motor Vehicle Programs
National Highway Traffic Safety Administration

Integrating a Multifaceted System Safety Program for a Large Complex System
Mr. S. W. Malasky
Manager, Assurance Engineering
Litton Systems, Inc.

Reliability Techniques in the Petroleum Industry
Mr. Henry L. Williams
Chief, CFE Engineering Branch of Reliabilility Division
NASA-Manned Spacecraft Center

System Safety Engineering in the Development of Advanced Surface Transportation Vehicles
Mr. Harry E. Arnzen
Safety Manager for Tracked Air Cushion Research Vehicle
Grumman Aerospace Engineering Corporation

Session VI Question and Answer Period

Observations and Reflections
Mr. Jerome F. Lederer
NASA Director of Safety

Closing Remarks
Mr. Philip H. Bolger
Conference Chairman

[redacted]

OPENING REMARKS

Jerome F. Lederer

NASA Director of Safety
National Aeronautics and Space Administration

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

OPENING REMARKS

Jerome F. Lederer

At the System Safety Conference three years ago to which Mr. Bolger alluded, we explained what system safety could do, we reviewed its early applications, and hinted at its potential. Then when Bob Helgeson summarized the conference, he said that system safety has come of age and it is time to consolidate the gains. We meet today to hear about the gains and view the broader industrial scope of system safety. I feel that one of the important gains is that its reception among engineers and executives is far better now than it was two years ago. To do this the engineers, executives and program managers had to surrender some of their instinctive feeling that they know all there is to know about safety; that therefore there is no need for a separate discipline on design or operational safety, no need for a well-prepared plan of checks and balances to combat the elements that are antagonistic to the identification and control of undesired events. Some of these antagonistic elements are meeting schedules, cost constraints, production problems, performance, and the "not invented here factor." Dr. George Mueller, who at that time was head of the Office of Manned Space Flight, stimulated system safety by defining system safety as "organized common sense." The Office of Manned Space Flight Safety in 1967 recognized system safety as a separate discipline and prepared the Apollo Program System Safety Directive. System Safety has since become part of the NASA Safety Manual and the concept is spreading throughout NASA. System Safety means the identification and control of foreseeable hazards as well as the documented rationale of residual risks that have to be accepted. The historical role of safety was to take corrective action after the undesired event had occurred. Of course the lesson learned from the undesired events are required inputs to system safety. But we now try to act beforehand to prevent rather than react to a loss. The old-fashioned waiting for an accident and then taking corrective action is commonly referred to as "tombstone" safety. The problem of trying to foresee the hazards to prevent them is a grand strategy directed towards curtailing losses throughout the life of the hardware. This is in contrast to the old way of doing things, which was the tactical approach of waiting to search and destroy the immediate enemy (accident when it occurred.) We now try to foresee these undesired events through system safety. We of course favor the strategical approach in place of the tactical approach though both of course are necessary.

The constraints of schedule, cost, performance and production which I mentioned before and even public pressures must be included in the grand strategy. Hazards are not limited to hardware. They include software, procedures, awareness. All assumptions on which decisions are based should be recorded for periodic review. System safety comes at an opportune time. Risks of great magnitude are increasing. This may mean a single risk such as an Apollo or the Alaska pipeline or it may mean millions of people exposed to individual risks as on the highways or the railways.

As management of industry or government projects becomes more beset by the political, economic or loss of prestige implications of mission failures, they will be impelled to turn with increasing attention to the systematic approach to loss prevention known as System Safety.

In his welcome remarks at out first conference, Dr. John Clark, our host, had some words of wisdom. I'd like to quote them. He said, "In order to sell the project manager on the necessity for integrating safety into the total program, he must be sold on the idea that project safety is synonomous with project success." A specialist in the field of safety is needed to look after safety, to help line management, to handle the whole safety job, not do it with their left hand, so to speak. Both groups must work together. Safety should be instituted in the conceptual design, before hardware design is started. One has to build in safety at this point if there is to be a good chance of achieving it further downstream. Then when the prototype hardware is ready to

go into test, make sure the testing is adequate. This can be a hazardous procedure. It is a time when one must be very careful to integrate the safety plans with a review of the adequacy of the total system.

There are very powerful forces that are pushing for the acceptance of system safety. The most prominent force is the adoption of system safety by Government agencies, the Department of Defense, NASA, Department of Transportation, Federal Aviation Agency. The consumer movements spearheaded by Government agencies such as the National Commission on Product Safety, the Special Assistant to the President for Consumer Affairs, the Highway Safety Act, the National Transportation Safety Board, as well as non-Government consumer protective groups, all are acting in such a way that guarantees the future of system safety or its concept by whatever name it is called. I prefer Risk Management.

In the home product field last year there were 30,000 people killed, 20,000,000 injured, a total loss of $5.5 billion. This shows where system safety has scope in fields other than space and aviation. The new Occupational Health and Safety Act will create a safety climate that will reach down to the smallest business enterprise, when the Department of Labor begins to enforce its standards. Self-defense will compel industry to adopt the system safety approach for the industrial type of accident prevention, including fire. Another very powerful influence for promoting system safety is the insurance industry, especially that part of the insurance industry that writes product liability insurance. The costs of law suits and settlements are becoming ever larger. The best defense for industry is proof to the jury that it has made a well organized and documented attempt to foresee and deal with identifiable hazards. The Kemper Insurance Co. of Chicago has put out a book called "Product Liability" which tells its insured how to protect themselves in the case of a law suit. This little booklet is just another definition of system safety. Incidentally, it includes "motivation" which sometimes is forgotten in the system safety program.

With these forces pushing system safety ahead, I foresee a fine future for it. The marriage of management with risk analysis, safety engineering, test procedures, will save much suffering and untold billions of dollars by putting hindsight where our foresight should be. It may be difficult if not impossible to prove such gains have been made, but we should all watch for them so that when we have this conference in 1974 you will be able to report on them.

I quoted some words of wisdom from Dr. John Clark, our host, I would now like to introduce him.

WELCOMING ADDRESS

Dr. John F. Clark

Director
Goddard Space Flight Center

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

Thank you Mr. Bolger, Congressman Pettis, and Ladies and Gentlemen. Good Morning and welcome to the Goddard Space Flight Center.

We are pleased to again host the Government-Industry System Safety Conference here at Goddard. We hope your meeting will be successful and your stay in the Washington area will be pleasant.

I noted from the Program that you will have many interesting topics and able speakers during the next few days, and I hope to be able to drop in from time to time to hear some of the sessions. I understand that Goddard is represented by approximately 50 members of our staff and so I am sure your discussions will impact the Center's thinking.

At the last conference I made three points which I felt were basic to the promotion of safety programs. The first is the necessity to persuade the project manager that project safety is synonymous with project success. Second, that a team approach between the line manager and the safety specialist is necessary to detect the unanticipated hazards, the ones that hurt us most. Third, that a formal system is required to bring the safety specialist and the line manager together during at least three phases of a project; the review of the conceptual design, review prior to the testing of prototype hardware and during the Flight Readiness Review.

It seems to me that these elements are just as applicable today as they were three years ago. Today, however, with the theme of this conference being "Applications and Experience" gained since the last conference, it might be prudent for me to explore this idea further and discuss the application of these ideas. Clearly, System Safety has a place in Manned Flight, but for unmanned missions some feel mission success is more directly dependent upon reliability and quality control functions. This seems to me to demonstrate a lack of understanding of what system safety is. There is an excellent short article in the September 1970 issue of Machine Design entitled Spotting Trouble Before It Happens which puts this comparison into language that a project manager might readily understand. The article compares fault tree analysis, frequently used as a systems safety tool, with failure mode analysis long used as a reliability function tool. An analysis which begins with the definition of an undesired event and works down from the highest level subassemblies may well point up risks which a method that begins at component level may not.

Development of the team approach between the safety specialist and the line manager requires mutual respect and confidence between the two. In practical application, it must be understood by the line manager that safety is his responsibility. It cannot be separated from his management functions any more that coordination or decision-making can. The safety specialist's effort, therefore, must be in addition to this line management responsibility, not substituted for it.

My third point stressed the importance of including in the review cycle at various stages assurance that collaboration between the safety specialist and the line manager takes place. I think this straight-forward concept requires little explanation. It is important, however, to extend the review beyond just hardware systems. The operations performed by people must also be considered. At Goddard prior to each Apollo mission we have our medical staff review the records of our key personnel to assure that they have inoculations for virus and other prevalent illnesses as well as a recent physical. In addition, we try to provide contingency plans to cover the emergency absence of a key figure. We try to expend adequate thought and analysis to determine back up requirements to eliminate the necessity for individuals to work extended shifts which might tax their efficiency. These are examples of the type of personnel systems review that needs to be addressed in addition to hardware review. Responsible managers must provide positive assurance that their personnel systems are as error-free as is their hardware.

In keeping with the theme of this year's conference, I have tried to elaborate on my opening remarks of three years ago, expand them and speak of their application. We hope that conferences such as this will help lead the way toward not only application of known principles but in exploring the frontiers of the state of the art of risk management.

Thank you for honoring the Center by your presence. We hope you will have a successful and enjoyable meeting.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Government-Industry System Safety Conference

Goddard Space Flight Center

KEYNOTE ADDRESS

by

Honorable

Jerry L. Pettis
Congressman - California

May 26-28, 1971

Thank you, Mr. Chairman, Mr. Lederer, distinguished speakers, ladies and gentlemen.

It would be presumptuous of me to try to tell this audience anything about System Safety. You are the experts on that subject. I'm sure you'll be even more expert after you've been exposed to the excellent program that NASA has assembled here for you.

However, I am vitally interested in all aspects of System Safety. My years as a commercial pilot instilled in me a profound respect for any policy, procedure, or system that would contribute to the improved safety of my passengers, my airplane, or myself.

More recently, my years of service on the House Science and Astronautics Committee have enabled me to appreciate -- at first hand -- the unprecedented hazards, both on the ground and in space, that have been generated in the Space Age as we have responded to man's eternal challenge to explore his environment -- and to satisfy his always urgent need to know. I have seen the magnificent response by creative and dedicated program managers and safety engineers -- like many of you here -- who have worked together with your partners and associates in industry to make space travel the safest mode of transportation developed for Earth men -- so far.

You know, I think it's safer to be on an Apollo flight crew than it is to be in Congress these days -- what with bombing the Capitol building -- the May Day demonstrations -- and the recent threats to stop the normal functions of our national government. If we can't make our governmental systems safe, how can we ensure the safety of our citizens? How about some of you working on System Safety Capitol Hill? I don't believe it would be any tougher than making the Apollo Saturn safe.

At any rate, since I'm not a Safety Engineer, I thought I'd talk about the application of System Safety Principles toward the solution of planetary problems. American space travel via Mercury, Gemini and Apollo -- has proven that we have learned to control the hazards we've encountered. Space travel via Planet Earth -- throughout recorded history -- has proven much more difficult. We might almost say that the hazards seem to have controlled us. Surely, we can learn to do something about that. If we could put six Americans on the moon, we can do anything -- if we care enough to try.

The System Safety concept -- the principles and the professional know-how -- may be much more important than we've realized.

I am aware that the theme of my address may seem to be a little bit pretentious -- "System Safety -- Planet Earth". Are we ready for it? How much longer can we do without it?

What I'd like to do today is to expose -- and try to clarify -- a concept. The concept is relevant to this conference because the principles of safety -- especially when applied with the expertise of systems management -- are of universal value.

This gathering is symbolic of a much larger society. You represent many aspects of our national life. We have in America a complex system of government, purposely representative of all elements of our modern civilization. Among you here today are safety-oriented leaders from diverse industries, colleges and universities, and a wide spectrum of government agencies. Over seventy different types of groups can be identified. More specifically, you are professionally interested in all armed services, all modes of transportation and the national space program. The AEC, HEW, FAA, Interior, the Post Office Department, the TVA, the Library of Congress, the GSA, the National Bureau of Standards, the National Transportation Safety Board -- as well as the District of Columbia and other Community and State governments -- are all here.

It's safe to say that most of you are professional safety engineers, or managers with safety responsibilities. Your common interest provides a common bond. It has brought you together with NASA as the catalyst. Mutual interests and responsibilities motivated you to join us here today. Why?

Why are we so interested in safety? Because it's our job? Or do we believe in -- are we dedicated to -- the principles behind the safety concept -- the preservation of human life, the conservation of materials, and the assurance of mission success?

Were you taught that Self Preservation was the first law of Human Nature? I was. The traditional right of self defense -- for an individual or a nation -- derives from that fundamental Law of Self Preservation. There is an even more basic law in Nature -- related

to the instinct to survive -- to grow to maturity -- and to reproduce in kind. Survival, defense and preservation of self -- are directly related to the safety concept.

The concept of freedom seems to be a natural extension -- or a more evolved development -- of that Law which recognizes that a man must live in freedom truly to preserve himself. We've tried to develop a way of Life in America that provides the best possible environment -- and the safest -- in which to live and grow. National Safety is also National Security.

We recognize "inalienable rights" that protect individual freedoms to live and grow -- as long as those rights are not distorted into license -- to deny another's freedom or his rights. This freedom or these rights are never relevant, unless we value the individual units of society as being human beings. Rights and freedoms become meaningful only if we value the human being and his native rights -- to live, to grow, or to become responsible for his own choices.

Our founding fathers were concerned with safety. They believed in the value of a human life. They even believed that the principle of freedom was inherent in a Law of Nature conceived by Nature's Creator. Whether we share that belief, it is undoubtedly the reason that Americans, traditionally, have set high values upon human life, their own or someone else's.

For nearly 200 years we have believed in this principle so much that we have often risked -- and even sacrificed -- our own lives, that others, weaker or more threatened than we, could also share the "blessings of Liberty".

What does this have to do with System Safety? Well, we sometimes refer to our "system of government", or even "the free-enterprise system". But more "right on", perhaps, the value of the life is essential to the safety concept. If life has no value, why protect it?

But we don't always obey law -- even a Natural Law. We are just beginning to recognize, on a planetary scale -- thanks to our Space Age perspective -- some of the awesome problems that we face when we disregard or disobey the laws of nature. "Self preservation" now pertains to all humanity. Planetary Security is directly related to the essential natural resources of our planet.

Self Preservation is inseparable from global ecology. The planetary system environment and our own viability as a part of that system are totally inter-related. They always have been. But we are now becoming very aware of this vital relationship. Conservation has now become an urgent mission, not just a part-time past-time.

Politically, the current problem seems to be, how to work for conservation without appearing too conservative.

I understand that three years ago you held the first of these System Safety Conferences. It must have been extremely successful. Look to what has been accomplished in those few years.

We've landed three Apollos on the moon. Six men from Earth have leaped around in moon dust -- and even "mulligan" -- and have returned to share unique experiences with Earth-bound men. Leaders like Jerry Lederer, Phil Bolger and their safety teammates must get due share of the credit -- as should all of you who helped them. A very special mention should go to a canine astro-pup called Snoopy -- perhaps the most successful safety engineer of all. Magnificent "mission success", shared with all humanity -- in the face of unprecedented risk to life -- with fantastic operational hazards to be overcome.

The tremendous learning experience of Apollo 13 may have been the most impressive of all -- in retrospect. The whole world was able to appreciate what value we placed upon the lives of astronauts. Perhaps we came much closer to the realization of System Safety Planet Earth as a result.

Of course, human life, primary though it is, is not the only safety consideration. There is the economy of resources -- of time, energy, money, and materials -- of equipment and facilities -- that is always at stake and riding with the mission -- not to mention the maintenance of public support for our manned space program itself. In this total light, the Safety of the System becomes paramount.

How can the uninitiated ever appreciate the value of the system safety concept? It really isn't easy. That may be why travel through space on Planet Earth has been so hazardous. It takes experience and intelligence. Wisdom is better -- though much more rare. It takes discipline and training and knowledge combined

with skill. But even more, it takes alertness -- or "awareness" -- and a very special kind of caring that produces individual responsibility. It all adds up to what can be called -- "Human Reliability" -- the most essential ingredient in any mission.

Instinct helps but we can't fly to the moon by the "seat of our pants". That seems to be the way we've been "piloting our planet".

But it wasn't instinct that permitted man to fly. Our physical bodies weren't optimized for flight. We had to learn to counteract the effects of the Law of Gravity -- or, more accurately, we had to learn to cooperate with a Natural Law that we call "gravity" in a way to make manned flight feasible.

I recall many steps in the process. Ground school training -- the flight simulator -- flying, with an instructor -- the dual controls -- level flight -- take-offs and, you hoped, safe landings, and finally -- the solo. Then more difficult maneuvers -- instrument flying, in worse than "field-grade" weather -- and the responsibility for other lives in an aircraft under your control. And then, an entirely different set of standards for piloting commercial passengers -- on scheduled flights.

The basic idea of System Safety was inherent in the training of a pilot from the very first day. You were taught to recognize different kinds of dangers -- like the approach to a stall -- or entering cloud or turbulent formations. You had to achieve the unnatural discipline of total reliance on instruments. You learned that most fatalities were caused when pilots ignored the "envelope of danger". That's just as true today. I still fly my own airplane and I still have to obey all the rules. You're particularly aware when you have your own family on board. Airline passengers take it for granted that the pilot is behaving like a System Safety Engineer -- on duty -- and totally aware.

Space Flight has forced us to advance and accelerate the state of the art of System Safety. The System Safety process involves an orderly understanding of the hazards to be encountered -- and the development of reliable ways to control them. There is a lesson here for solving planetary problems.

Whether it's ground safety, industrial safety or flight safety -- 99% reliability isn't good enough -- not any more -- not with an astronaut on board -- not with so much riding on the mission.

Space flight safety provided more complex problems to solve -- but the principles were the same. And all through the process -- the priceless ingredient was always -- and will always be -- what might be called, the Human Reliability Factor -- in the careful identification and evaluation of hazards -- to human life -- to the economics of time, materials and money -- and to ultimate mission success. The principles apply to humans and to hardware. People make the hardware. People use the hardware. People must control the environment or the environment will control the people.

All these factors directly affect the "viability" of the System -- and the viability of any "human systems" whose lives are risked. The human systems, at least to us, are the most priceless of all subsystems.

We recognize now that system safety must be foremost in the minds of managers throughout all phases of research and development programs as well as during operation of the systems. We recall the historic battle -- (or was it the kingdom?) -- that was lost for lack of a horseshoe nail.

During your last Conference, three years ago, Dr. George Meuller described System Safety Engineering as being "organized common sense". I'll buy that -- but common sense seems to be getting more uncommon every day.

There are some bright spots though and I'd like to reflect a little light from one of the brightest. I'm sure all of you have heard of "Spaceship Earth" by now. It's a useful, though rather challenging concept being effectively expressed by its inventor, Buckminster Fuller. (I'm sure the more "pragmatic" types would label it "simplistic".)

"Bucky" Fuller, now an energetic 75 or so, recently wrote a book called "Operating Manual for Spaceship Earth". Since then he has also invented and developed the "World Game". I'm sure Fuller has defined the patterns related to "System Safety Planet Earth" better than I could. He thought about the concept and understood our planet Earth as an integrated system -- a long time before the Apollos made their impacts on our minds and hearts.

Fuller is optimistic about our chances for safely piloting the passengers and crew of Spaceship Earth into a more creative,

harmonious and prosperous future -- if we put our best minds and strongest wills to accomplish mission success.

Buckminster Fuller is not just a dreamer -- although he's not afraid to dream -- or to make full use of his fertile imagination. He has assembled impressive credentials. Fuller has developed more than 150 separate patents in 58 countries of the world. 10,000 of his geodesic domes -- like the one assembled at Expo 67 -- are scattered over the glove. His name has 26 honorary degrees tagged on behind it. He's a multi-disciplinary systems-management task force, all in one -- being simultaneously described as architect, cartographer, cosmogonist, designer, engineer, inventor, mathematician, philosopher -- thinker and problem-solver -- and even a poet. He's young and very idealistic, for his age. How can we train more "specialized generalists" like Bucky? When asked to describe himself, Fuller says, "I am a random element."

Are you wondering whether Bucky Fuller is relevant to a conference on System Safety? I think he is. Just as relevant as a conference on System Safety is to the mission success of Spaceship Earth.

We understand that System Safety Engineers must consider carefully all aspects of the environment in which the system is to operate. Recently, we have learned something about the hazards in space. We have also learned -- through costly centuries of history -- something about the hazards on board Spaceship Earth. On a planetary scale, we haven't learned enough yet about hazard analysis, risk avoidance or over-all systems management. We have a long way to go toward controlling our environment. We are just beginning to understand the Life Cycle of the System. Our essential feedback is all too often -- distorted, garbled in transmission or completely blacked out.

In accordance with the System Safety approach, could we revise the mission to reduce exposure to hazard and minimize our risks? Revise the planetary mission? Perhaps -- if we knew what our mission really was. That's been the age-old riddle for mankind to solve. Unless we know our purpose we never can define what's "relevant". If you don't know where you're going -- or why -- how do you know what to take along -- how to train yourself -- or what kind of guidance you will need?

Maybe when we see the world, as Bucky Fuller does, as a complex unity -- of interrelated and dynamic systems -- we might give better thought to the original System Designer -- and try to discover and define His system concept. If He didn't have mission success in mind -- then nothing has much meaning. And if -- He was capable of designing -- even the simplest atom -- and setting it in motion -- then He could have had in mind a perfect System Safety plan for us to follow.

The traumatic and inspiring experience of Apollo 13 now can be given profound symbolic meaning. The life on board became vitally important to millions of fellow passengers on Spaceship Earth. For a few moments in history we glimpsed the highest priority. The support crew focussed on solving the most urgent problem -- and succeeded like seasoned professionals.

Can we ever keep our planetary passengers safe? Can System Safety Planet Earth ensure ultimate mission success? Or will the immaturity and irresponsibility of some of the crew members prove fatal to the mission? Will some of us -- always be willing to escalate the risks and amplify the hazards -- like playing "chicken" on a planetary scale -- using risk as a weapon system with which to threaten, intimidate, and take over the controls of Spaceship Earth -- in a ruthless attempt to hijack -- willing even to abort the mission unless they can command the ship -- absolutely -- once, and for all?

To enjoy life on Earth as a "viable humanity" -- "capable of sustaining life and growth" -- we must also maintain a viable planetary system. To achieve mission success we must first identify our mission on this planet. When we begin to even understand that question and to formulate a "common sense" approach to find the answer -- only then will we begin to be secure -- for the first time in all of human history.

PERSPECTIVE FOR SYSTEM SAFETY

Honorable

Willard J. Smith

Assistant Secretary
for
Safety and Consumer Affairs
Department of Transportation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

I was pleased as well as honored when Jerry Lederer invited me to deliver the "kick off" remarks to this Second Government-Industry System Safety Conference.

To those who have been working on development of new and sophisticated hardware, the notion of a systems approach to problem solving is old hat. Everyone in NASA understands what is meant by a systems approach and that is surely an important reason why this Second System Safety Conference can be addressed to applications and not to continued discussion of what is meant by a "systems" approach to safety problems.

As Assistant Secretary for Safety in the Department of Transportation it is a function of my office to try to help lead the Department in the safety area. I believe the systems approach to safety problems can make significant contributions in improving transportation safety. The infusion of systems concepts and thinking into the overall approach to safety programs will, in my judgment, be of benefit to all concerned. I'm certain I won't have any difficulty selling the idea of a systems approach to transportation safety to this group. I am sure that my colleagues in the Department of Transportation are equally interested.

Although the Department of Transportation is four years old the decision was only recently made to establish a single, high-level advisor with Department-wide responsibility for safety coordination. The Secretary expects me to assist him in establishing uniform safety policies and practices throughout the Department and to help him evaluate the responsiveness of our safety programs to the public need. He outlined my responsibilities quite clearly when he said, and I quote:

> "The Department's safety programs are now administered under differing philosophical and procedural concepts. Some of these differences are caused by the various statutes which created the programs and some have been a matter of administrative choice. I believe that all of these safety programs, although administered by different elements of the Department should be administered under uniform policies to the extent possible."

In short, what the Secretary had in mind was that the Department's safety programs be regarded as a unified transportation safety system. It is an important part of my office's function to help lead the Department toward development of a unified, consistent, systems view of transportation safety.

Before discussing the kinds of systems safety activities that we are considering, it's worth taking a few moments to examine what is now being done. I cannot over-emphasize the importance attached to safety within the Department of Transportation. The legislation which established the Department specifically requires that it develop "national transportation policies and programs conducive to the provision of fast, safe, efficient, and convenient transportation." The word safe, which is strongly emphasized in the legislation, is given utmost attention throughout the Department, and continues to grow in importance.

Each of the major operating administrations within the Department has one or more of its key offices devoted exclusively or almost exclusively to safety. The Federal Highway Administration has an Associate Administrator who is responsible for Motor Carrier and Highway Safety.

The Coast Guard has key offices responsible for Merchant Marine and Boating Safety.

And the Federal Railroad Administration has a Bureau of Railroad Safety.

These are all positions at the highest levels within their agencies. Safety is, of course, what the National Highway Traffic Safety Administration is all about. To a very great extent, the same is true of the Federal Aviation Administration. The Offices of Hazardous Materials and Gas Pipeline Safety are pure safety regulatory organizations.

The National Transportation Safety Board, created by Congress under the Transportation Act of 1966, has broad powers to recommend safety practices in all modes of transportation. It determines the probable cause of accidents, and proposes corrective actions through safety recommendations.

Secretary Volpe has clearly indicated that the operating administrations within the Department shall retain their safety responsibilities. However, he expects my office "to assist in the development of more comprehensive, coordinated and cohesive vehicle and system safety programs in and among the operating administrations."

The preceding comments indicate thc very high priority given to safety in the Department of Transportation. The presence of several speakers from our Department at this meeting is further witness to the importance we attac' to safety. I know that excellent system safety efforts are going forward within individual modes of transportation. But I am far less certain about our basis for determining how safety resources and efforts should be allocated among either competing programs within individual modes, or among all of the modes.

I feel confident that we do a good job of applying systems safety skills to particular problem areas. But I have doubts about the perspective with which we allocate our systems safety resources among the numerous demands on these resources. I will try to illustrate this point with several examples of situations tnat we face within the Department of Transportation.

Consider that motor vehicle accidents account for over 90 percent of all transportation fatalities in the United States. As a result, a one percent increase in the motor vehicle death toll would have an approximately equivalent effect on total lives lost as a 10 percent increase in the combined death toll from all other causes of transportation fatalities. Viewed the other way around, if we could reduce motor vehicle fatalities by one percent, we would save roughly the same number of lives as we would if we reduced fatalities in all of other modes combined by 10 percent. This simple illustration poses what should be an obvious question. Namely: What are the relative results of safety improvements in the various modes of our transportation system? And, are we making our transportation system safety investments in ways that promise to maximize the number of lives saved? I'm not convinced that the answer to such questions have been explicitly worked out or furnished to the Secretary of Transportation.

It seems clear that the answer to such systems safety questions would place the Secretary in a better position to make decisions on allocating the Department's safety resources among the several modes. I have a strong suspicion that such questions go unanswered in many Government agencies. We, as safety specialists, should be concerned that answers to such broad systems safety questions are provided -- or, at least, that the questions are explicitly raised.

Comparing 1970 with 1969, there was a 2 percent decline in fatal transportation accidents. This decline was dominated by, and principally reflects, a 2 percent decline in motor vehicle accidents. However, in 1970 accidents either declined or held steady in all modes of transportation. This occurred despite considerable growth in transportation usage. Aviation fatalities declined by about 10 percent, and railroad fatalities declined by about 5 percent. At the same time, the two other major areas of transportation fatalities--marine and grade-crossing accidents--remained roughly unchanged.

Such comparative data pose an interesting question for Department of Transportation systems safety specialists to ponder. Could we, or should we, set ourselves arbitrary safety targets? For example, we could establish an objective that the number of fatalities in each transportation mode should not be permitted to increase. Such an objective would doubtlessly lead to wide disparities in the amounts spent for lives saved in different modes, and could probably not be justified on economic grounds alone. Nevertheless, information on the cost of such a policy objective would be of immense value to the Secretary.

Secretary Volpe recently testified before a Senate Committee that it is a Department of Transportation goal to cut in half by 1980 the number of people killed on our highways. This provides a specific goal for the Department of Transportation. The questions that its systems safety specialists ask are: First, what are the alternatives available for achieving this specific goal? Second, what are the costs associated with each of these alternatives? Some of these costs will be measured in dollars, while others will be measured in terms of constraints imposed on operators of motor vehicles.

I believe there is an important need for development of information on the safety options available to agency or department top management, and on the costs associated with these options. In the Department of Transportation, the options should include such choices as holding the line on increases in accidents, or cutting accidents in half by some particular

time. This is the kind of information which will provide top management with perspective on their safety problems, and will furnish them with the material they need to go forward with safety programs. It is my impression that such information is now sorely lacking in many, if not all, government agencies.

My office has been assigned the responsibility for initiating work on development of a series of goals and objectives for the Department of Transportation safety programs. Initial steps in carrying out this assignment will involve making forecasts of the number of accidents that can be expected in each of the several modes of transportation, and of examining trends and accident rates. Thereafter, it will be necessary to consider possible accident reducing measures as well as the savings that will result from the reduced accidents.

As I have tried to emphasize, this is the kind of information the Secretary needs for all modes of transportation. He needs to know a great deal more about the cost and results of system safety improvements. He has no choice but to view the safety problem in the perspective of costs and benefits. As safety specialists, we should also try to view the problems this way. Then we will be in a position to provide our bosses with the information they need.

We must approach our problem broadly. Thus, analyses of means to reduce automobile accidents is not limited to such considerations as the building of better roads and more crashworthy cars. It also examines such options as expenditures for improvement of traffic law enforcement. Or for more prominently advertising the dangers of drinking and driving. Or for improving (and perhaps subsidizing) state auto inspection programs. The point is that reducing automobile accidents is a systems problem in the broadest sense, and the mechanical steps that might be taken to improve the situation should be viewed as nothing more than segments among a broad array of alternatives. Indeed, these alternatives should include possible steps that might be taken to divert people from use of autos to use of far safer public modes of transportation.

Research now going forward in the Department of Transportation provides an example of systems safety analysis which, I believe, very nicely illustrates the kinds of broad perspective in which safety can and should be approached. Safety would be improved if travelers could be induced to use public transportation instead of their own autos. It is observed that common carriers are required to maintain a degree of safety far in excess of that in user operated modes. This high level of safety is ultimately reflected in the cost to the fare-paying passenger. On the other hand, the costs of the National Highway Safety Program have been largely borne by the public at large through general taxation. As a result of these actions, safety costs on private transportation are subsidized by the Government. Such governmental action tends to raise the cost of a public transportation mode, and to lower the cost of a private transportation mode. As a result, governmental action in this case tends to encourage a shift from safer public modes of transportation to a less safe private mode of transportation. Viewed strictly from a safety viewpoint, and one must remember there are other considerations, this behavior is possibly the reverse of what it ought to be.

I believe that a systems approach to safety can have its largest payoff in the broad area of development of safety policy. To be effective at the highest levels of government, systems safety analysts must learn to view our problems in the same terms as the top management of our agencies. We must also learn to work out the kinds of safety trade-offs that top management of our agencies can easily understand and easily utilize. We must become skilled at taking account in our analyses of the full range of options available. If we learn to do all of these things well, we will have contributed significantly to making America a safer place in which to live.

Thank you.

SESSION I

NEW DEVELOPMENTS IN SAFETY

Session Chairman - Mr. Philip H. Bolger

"Communication of Risk"	Dr. Raymond M. Wilmotte
"System Safety Management - A New Discipline"	Mr. W. C. Pope
"Data Requirements Analysis in Support of System Safety"	Mr. I. Irving Pinkel
"Reflections on System Safety and the Law"	Mr. Daniel F. Hayes, Sr.

INTRODUCTION

All decisions are based consciously or unconsciously on the balance between benefits and risk. That is true for all of us, at all times. I am going to discuss this balance, and for that purpose will divide applied technology into two parts· Benefit-oriented and Risk or Uncertainty-oriented. Benefit technology includes design, development, manufacturing or construction, operations. Risk or uncertainty technology includes safety, reliability, quality assurance, test, maintenance, as shown in fig. 1. This picture is key to the decision-making process. The process may be invisible, taking place in the decision-maker's mind from his knowledge of the problem, or at the other extreme, it may involve a process with independent benefit and risk departments supporting and, at times, confronting each other. But always the decision will be affected by the balance with which relevant information of the benefit and risk technologies have reached the consciousness of the policy maker and stimulated his interest.

It is the importance of this balance, its present and potential status that is the subject of this paper. The premise of the discussion that follows is that for decision and policy making at all levels, knowledge of the consequences of risk is as important as knowledge and consequences of benefits.

Perhaps the purpose of the paper is best depicted in the two cartoons of fig. 2 and 3. Fig. 2 represents current unbalanced benefit of risk presentations, while fig. 3 represents balanced conditions, more helpful to the decision maker.

The discussion of risk brings different things to mind to different people. Here, I use the term very broadly. Risk exists because one is uncertain about some things. These uncertainties could range in technology from areas beyond the state of the art, and lack of knowledge about the environment, to analyses and tests not made, capabilities not used, and human errors of all kind.

I treat risk and uncertainties as synonymous. Technically I prefer uncertainties - Risk implies a number, often of vague meaning. Uncertainty gives a sense of needing to know more and wanting to do something about it. Professionally I think uncertainty; for public relations and lay communication I talk risk - it seems a nicer, more generally acceptable word.

In addressing this subject to the safety community, I should point out that system safety is a most important part of the risk technology and holds a specially politically sensitive position in the eyes of management.

COMMUNICATION: A PRIMARY NEED

Nearly all engineers are dedicated to their work; system safety engineers are no exception nor are other types of engineers working in the risk technologies. But being trusted is not enough; we must justify our utility in the eyes of the decision-makers in relation to that of others who bear other technical responsibilities. It is not sufficient to argue the importance of the work; we must convey its value. It must be expressed in realistic terms and attractive form; and it must make it possible for the decision-maker to compare the benefit-risk ratio of alternative courses of action.

The responsibility for deciding how much risk to take is generally viewed as the exclusive province of top or near-top management. And indeed top management's activities are almost exclusively focused on balancing risk against benefits on a macro scale, but down the line innumerable risk-benefit micro decisions are made without knowledge of higher management. Some of these turn out not to be micro at all, and become known only when their effects become visible, sometimes too late for correction or late enough for correction to be costly.

There are a number of reasons for judgment to be slanted in favor of benefit, meaning that there is a tendency to take more risk than would seem desirable. This condition can be reversed following a serious accident or crisis. Then, for a while, exceptional attention is given to understanding risk and reducing it. But the full effect is usually temporary. There is a natural tendency to return to the state of mind that existed prior to the crisis, to degrade or even forget some of the "lessons learned." The trend rapidly accelerates as the team that lived through the tense atmosphere of the crisis is dispersed among other programs. Some procedures which were adopted may be retained but the degree of attention given to them tends

to drop, and the risk engineers have a harder time achieving effective communication.

Each type of risk activity includes a variety of steps, procedures and techniques, but they have a common ultimate purpose. It is to warn of the probability of impending trouble, the resources and time required to reduce that probability and reduce the probable damaging effects if it occurred. The warning is given to the appropriate levels of the benefit activity. With this information the decision-maker is in a position to decide whether the risk is sufficiently low to permit operation or whether it is preferable to take steps to reduce it.

The decision-maker's judgment as to the desirable benefit-risk ration depends on a number of considerations and their balance is affected by current material and political pressures. This judgment is a very personal matter. A gambler will under-value risk, a miser will overvalue it--at least from the point of the middle-of-the roader.

Facts and analytical logic limit the area within which judgment must rule. Outside this judgment area quantitative facts dominate. Experience shows that hard data tends to displace the soft and tenuous, even logic, sometimes with little regard to importance. In the soft area it often happens that the personality of him who presents the information has more impact than the information itself.

In most organizations which are not technically oriented, no group is assigned the specific responsibility of assessing risk; everyone is expected to know that risk exists and make decisions within the area of his productive responsibility in accordance with his best judgment. But does everyone at each decision level give consideration to the balance between benefits and risk? The answer is yes! Everyone does, but often it is done unconsciously with little conscious realization of the risk introduced. Seldom is the risk involved systematically communicated to higher management. The effect is cumulative; as one decision influences another the risks add, and many uncertainties -- assumptions, approximations, conflicts, etc. -- are lost to the decision-making process.

Expressed in this way, it would seem that current decision-making process is terrible. We know, however, that it is not so; decisions are on the whole good, except sometimes....

In technically oriented organizations, however, there exist departments specifically oriented to certain areas of risk. Some, like system safety and reliability, are mainly analytical; others like quality assurance and tests (of the qualifying and acceptance type) are largely processing. These areas provide information on uncertainties and tend to counteract the normal tendency to underestimate risk.

THINK-POSITIVE SYNDROME

The titles of the risk activities -- Safety, Reliability, Quality Assurance, Test, etc. -- appear on the doors of these department, but when one enters one hears about failures, accidents, defects and anomalies. Why? Because the terms "reliability," "safety," "quality assurance" and "tests" are reassuring, while "failures," "accidents," "defects" and "anomalies" are not. But professionally the specific work consists in reducing these uncertainties, and any effort to quantify them focuses on estimating the probability of their occurrence.

One can refer to these "risk departments" as "uncertainty control departments" as better describing the type of work. Risk gives one a sense of a number, often of uncertain meaning, while uncertainty brings to mind the specific elements that produce risk and even a desire to do something about each one. When uncertainty professionals talk to policy-makers they will use the terminology of their titles: they will state, for instance, that the reliability is .9992 and not that the probability of failure is 8×10^{-4} -- reliability sounds better than probability of failure, for the same reason that betting on a horse is based not on the probability of its losing but of its winning.

This type of phenomenon I have termed the "Think-Positive Syndrome."*

In industry, as in government, positive achievement is psychologically a must. As in the horse racing analogy, man loses interest in probabilities which involve considering losing rather than winning, even though the mathematical odds are not affected. Given the option,

*Wilmott, R. M. "Engineering Truth in Competitive Environment: IEEE Spectrum, Vol. 7, May 1970, pp 45-49

his interest will focus on benefits rather than uncertainties.

While the think-positive state of mind is essential to a program, it has some damaging consequences, the common basis of which is the tendency to unbalance the benefit-risk ratio in favor of the benefits.

The problems it engenders start with the statement of goals. These are mainly of the benefit type, most of which can be expressed quantitatively such as payload of so many pounds, cost so many dollars, schedule of so many days and equipment of specified physical characteristics to make measurements or observations. In the risk area the probability of failure is difficult to quantify. Numbers here, for reasons difficult to refute, are currently discredited. The desire to achieve benefit goals puts pressure to underestimate uncertainties and risk. The pressure is high because the goals are set at a level somewhat beyond the state of the art and risk estimates give way relatively easily because of the flexibility of current techniques for expressing uncertainties in numbers.

In one form or another the syndrome affects all stages of a program. It tends to make a whole organization lean toward giving more consideration to performance information (usually hard data) rather than to uncertainties (often soft or tenuous data) regardless of importance, or more pragmatically to lean toward underestimating rather than overestimating cost and time, and later in the program to sacrifice too readily risk-reducing activities to protect schedule and budget. The think-positive syndrome tends to make communication difficult and inefficient, because the analysis of risk inevitably focuses on uncertainties, which to the non-professional are negative aspects of engineering and management, although uncovering, assessing and doing something about them is clearly one of the most positive things an engineering group can do.

It is under stress, when funds and schedules are tight, when crises occur, that the undesirable features of the think-positive syndrome are most likely to be prominent. Under these conditions, the communication gap between policymakers and uncertainty engineers is particularly great, much greater than the gap that often exists with design and operations engineers. The pragmatic reason is that the latter are in a sense disposable. Design engineers are essential to build hardware, and operational engineers to operate it, but uncertaintly engineers are needed to point out how uncertainties could be reduced, but primarily only to help the policymaker with risk data and analyses; and policymakers have for centuries made policies without them. While a few managers, design and operating engineers are beginning to welcome the analyses and advice of system safety and reliability engineers, the majority find them to be a nagging interference with getting on with their work. They often consider that existing talent in design, operations and policymaking can meet substantially all such peripheral requirements. Under stress there is a great temptation to save money and time by reducing or even eliminating the risk departments.

Is it desirable to carry out such a policy? At first glance it would seem so, for in these areas there are no techniques which a design engineer would find difficult to understand and learn. Why, then, did such disciplines as system safety and reliability separate themselves from design engineering to a greater extent than such specialized functions as structures, thermal analysis, communications, etc.?

There are two reasons for maintaining risk and benefit technologies in separate departments. One is the importance to quality of the work interest of the individual worker and the other is the benefit that is derived from confrontation.

WORK INTEREST

The worker must be interested in his work for it to be consistently well done. If he has to cover two areas, in the first of which he has considerably more interest than in the second, he will inevitably give more than proportionate attention to the first. The difference is particularly noticeable when he is working under the pressure of a tight schedule. If consistently high quality is required, the two areas should be separated and given to different workers. The separation will have the advantage that each worker will become more knowledgeable in the area to which he has been assigned, but much more important is that each area will be the primary interest and will receive the

primary attention of a worker. This situation exists strongly in the relation between the benefit and risk technologies. Design engineers are typically much more interested in the outputs and techniques of design than they are in those of system safety and reliability; they are not, therefore, likely to have equal interest or give consistent attention to the risk area, if they are required to cover both.

In the attached table I have listed my impression of the relative degree of interest of five groups -- Management, Design Engineering and the three risk assessment groups -- Safety, Reliability and Maintenance. Primary interest is indicated by a dark circle and secondary by a grey triangle. The number 1 indicates a somewhat greater interest than the number 2. The major difference in the interest is between the primary and secondary. This difference is to be judged not by verbal opinions but by action, by the extent to which under stress the secondary interest will be sacrificed for the primary; the extent to which system safety, for instance, will be sacrificed for schedule or for payload carried by a spacecraft; the extent to which as insistent a demand is made and expected for competence in system safety as in design; the importance given to introducing system safety considerations at the initial, the conceptual, as well as in the later stages of a program.

The table also shows that in the process of policy making three factors -- cost, time, and key performance parameters -- dominate the uncertainty control areas and the non-key performance parameters. Is the status of uncertainty control in policy-making process low because uncertainty control is not important?

The answer is that it is important, often the most important element when the whole life of the unit is the criterion, but often it is not important for the short term. And one must remember the forces on the policy-maker. For him the short term dominates, and long term effects and goals are considered only when short term needs are not pressing -- and the latter condition hardly ever occurs. There are few fields in which risk technologies have a standing at the top decision levels equals to that of benefit technologies. One outstanding exception is the Office of Manned Space Flight of NASA.

Even this handicap of long versus short term in giving greater attention to uncertainties might be overcome in time, if the risk areas were to provide information important and useful to making policy. They can warn of danger, they can advise Design regarding improvement, but it is difficult for them to develop a basis for statements such as "The design has deficiencies which will probably cost $X over its life, which could be reduced by $Y for a cost of $Z and a delay of T." Without this type of information how can a rational decision be made? This is the hard kind of data which design engineers can provide. Uncertainty engineers tend to provide soft data; safety engineers often provide only a list of some of the things that could happen. As already stated, experience indicates that hard data displaces soft almost regardless of importance.

BENEFIT FROM CONFRONTATION

A passive organization stagnates. Confrontation is essential to achievement, to progress and innovation. It can also be destructive, if it develops into personal conflicts. Ideally it is controlled and has a strong element of cooperation toward a common purpose. I apply the words confrontative and conflict in the clash of opinions to imply different attitudes. I visualize confrontation as an objective presentation of differences. Conflict includes an element of emotion and antagonism. Confrontative is constructive, conflict is destructive. In complex programs there is commonly a clash between functional and institutional managers. The initial confrontative sometimes degrades into conflict. On the whole the clash is beneficial. But the most potentially valuable confrontation for effective decision-making is between the benefit and risk areas. It would seem important, therefore, to keep them separate, each one as fully integrated as other practical considerations permit.

KNOWLEDGE: DESIGN AND UNCERTAINTIES

We know what we can design with a considerable degree of confidence, and this knowledge is the stimulus that impels us to go ahead with a program. However, we know little quantitatively of the risk we take in making these decisions. We know how to process all

kinds of data, but while we have much data on how to do things, we have little on assessing risk. We have universally great confidence in the capability of those who design, but we look with a degree of suspicion on those who deal with uncertainties.

In the course of developing a system we are constantly reducing and deciding what uncertainties to retain. It would be folly to carry out all the analyses and tests we would like to make, but we should keep in mind that whenever we decide to eliminate something, some analysis or test, we are increasing the uncertainties. At the end of the process, in our review of what we have done, we should include also what we have not done. Otherwise we can hardly judge what uncertainties remain. The uncertainties that remain are never zero.

Uncertainty is made up of a lot of little things. It includes also big, clearly visible problems, but these are usually, though not always, well recognized and taken care of, but the little ones slip by and can easily be neglected or even deliberately disregarded, and the sum of them can be far from negligible. For that reason, developing statistics is often difficult. In the case of system safety, for instance, the number of accidents due to a specific deficiency during a particular operation may be too small for meaningful statistics. In operational anomalies, however, there lies a huge fund of valuable data largely unused. They could be aggregated, listed with their source, cause, and the analysis, reviews, tests, inspection where they could or should have been caught. We should not over-concentrate on major mission failures; other anomalies are just as important real-life data to support future design, reduction of uncertainties, risk assessment, and decisions and to select, on the basis of their efficiency, uncertainty removal techniques - analysis, tests, reviews, etc. Applying such data to analyses of the type of failure mode and effects, one could develop quantitative, occurrence estimates of the conditions that could produce accidents. We would then begin to derive some sense of the probability of accidents taking place though none had yet occurred and even before a system was put into operation. A substantial and effective data bank of derived uncertainty information might thus be built up.

The development of this technique and the building of such a data bank would change radically the importance and policy status of the uncertainty technology; it would rehabilitate the status of the "numbers game;" it would bring estimates of risk, of the consequence and penalties of potential deficiencies and uncertainties of a program to a level of management appreciation comparable to that of the projected benefits. Management would then at last have balanced information on benefits and risk, without which decisions have to be largely a matter of unsupported judgment. We can even consider that contractors could be induced to establish risk during the development of a complex system in some systematic manner, so that both he and the buyer can assess and monitor the true progress of a project at each of its critical stages.

CONCLUSIONS

No specific formula is presented on how to introduce into an organization the principles I have outlined regarding the utility of the risk technologies and their relationship to benefit technologies. Clearly the best operation will vary greatly with the industry and its current pattern of operation. Moreover, it is by no means obvious where improvement would be cost effective. Intuitively one can expect only slow advance in the science of risk technology while it remains fragmented. Strong advance could be expected by integrating its several elements into a single department with its manager responsible for warning of dangers arising out of uncertainties.

The importance to quality of worker interest and the value of confrontation points to the importance of separating the management of risk and benefit technologies. There is no clear argument, however, whether raising the level of efforts of the risk technologies would be beneficial or not.

Looking back over this discussion one cannot help but feel that in its development, its data base and the degree of attention from management, risk technologies lag far behind benefit technologies. The lag in these areas is undoubtedly the reason for the greater attraction that benefit technologies have for engineers. That lag of itself does not justify

an increased effort in the risk area. Judging from the experience of some of the large programs one could reasonably come to the conclusion that adequate attention is being given to uncertainties, even taking into account the details of performance achieved, the anomalies experienced and the risks that they imply.

I have outlined a number of arguments describing existing conditions and pressures which lead to underestimating risk. All seem valid, but what value would accrue if these areas were improved, it is difficult to judge. The gain might indeed be little, but also it might be considerable. One might expect overall performance of many large programs to be sensitive to the quality of the decision process. If that is so, a small improvement should produce valuable results. Among the critical parameters of control one would expect to include risk at a level of attention no less than that given to any other parameter, including schedule and cost, and traded off on some reasonably comparable basis.

There is probably no controversy that an increased knowledge of risk in complex systems would help decision making. The controversial question is whether the improvement warrants the effort. Many managers feel that the present decision process is satisfactory; others don't. Among the latter is Undersecretary of Defense Packard. The fact is that we do not know; neither do we know what increased risk we incur when, under tight budgets, when crises are more likely to occur, we reduce the level of effort in the uncertainty areas.

It seems important to develop a better sense of the benefits that knowledge of risk could provide via the decision-making process. To carry this out will require an improved data base. By experiment and analysis on the effects of increasing the contribution of risk technologies, one could develop a better understanding of their potentiality and limitations.

The analysis in this paper has been written mainly with the idea of clarifying to technologists and analysts the place of the risk technologies in the managerial environment. Can it also indicate to management a possible line of approach to some of its needs? Judging from the demand of other countries for American management expertise we can reasonably consider ourselves equal to the best and possibly generally better in this field. But the urge for progress is in our blood. How do we progress in a field without guide lines, without goals, without means of measurement? The process we have followed is first to recognize some weak spots in our operation, and shortly sure enough, some ambitious top management tries an approach different from the current pattern for its type of operation. Whether it is an improvement or not is a matter of opinion, for it is almost always impossible to measure. Success is usually more felt than proven. To make such a move is generally dangerous to the individual, for criticism of managerial inovation, overt and covert, from managerial peers are easy to make and likely to abound, while praise comes more reluctantly. Experiments are difficult to carry out, for administrative changes may be strongly resisted by special groups and managerial levels. They generate barriers born of insecurity and fears - fear of being measured, of loss of authority and of freedom of action. The whole field is replete with prejudices and protective mechanisms.

So described the environment does not seem well suited to embrace a search for progress. Yet, these barriers are constantly being overcome, for progress has come consistently. This paper points to an area which is ready for progress. I believe it is a most important area, one in which a quantum step of progress can prehaps be achieved. The discussion of the paper was focused on technology, but the key element - the unbalance between benefits and risk in the decision making process - elements far beyond the boundaries of technology. If a systematic attack is to be made on this unbalance, technology is the logical first area to approach, for there the problem is most clearly definable, and its individual risk areas are well stocked, though still inadequately, with data, techniques and expert personnel.

My personal but unsupported opinion is that risk technology is a great and coming field. Advance there is needed more than in other technologies. It is not only needed in the hard area of engineering, but even more so in the soft area of the social sciences. It is rapidly changing from an art of judgment to a technology where we can begin to see the possibility

of reliable numbers based on physics and real life experience. We still have a long way to go before we can approach the values that this technology could provide. Risk assessment, supported by data and techniques for prediction, are receiving rapidly growing attention in many fields.

I would like to add one final opinion applicable to both the public and private sectors:

If one does not include throughout a major project a systematic uncovering of uncertainties and at each major milestone a thorough official assessment of risk, one probably loses one of the most important benefits for the future the project can provide - developing real life statistical data and learning how to apply them to decision-making.

We still have much to learn!

UTILITY OF RISK DISCIPLINE TO MANAGEMENT

- PURPOSE OF RISK DISCIPLINES
  - ADVISE HOW TO REDUCE UNCERTAINTIES
  - WARN OF PROBABILITY OF IMPENDING TROUBLE
  - FOR DECISION PROCESS: ESTIMATE RESOURCES AND TIME REQUIRED TO REDUCE THAT PROBABILITY AND ITS DAMAGING EFFECT IF IT OCCURS.
- DECISION PROCESS
  - BALANCE BENEFITS AGAINST RISK.
  - REVIEW BENEFIT AND RISK-INFORMATION.
  - FILL GAPS ON BASIS OF EXPERIENCE AND APPLY JUDGMENT.
  - DECIDE WHETHER TO CONTINUE OPERATION OR REDUCE RISK.

FIGURE 2

THE BALANCE BETWEEN BENEFITS AND RISK

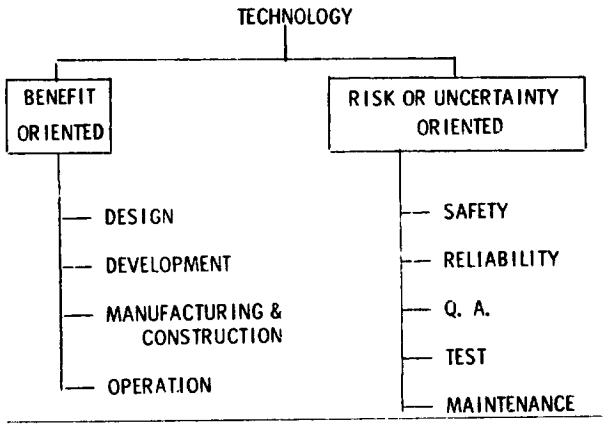


FIGURE 1

FIGURE 3

THINK POSITIVE IS A MUST IN ORDER TO

- PREVENT STAGNATION
- MAINTAIN INTEREST
- STIMULATE DESIRE FOR ACHIEVEMENT, PROGRESS OR INNOVATION

BUT

IT PERVADES ALL LEVELS OF AN ORGANIZATION AND UNBALANCES BENEFIT/RISK DECISION RATIO:

EXAMPLES:

AT START		
HARD PRESSURE TO ACHIEVE DIFFICULT GOALS	VS	SOFT CAPABILITY OF UNCERTAINTY ESTIMATES
UNDER STRESS		
DESIGN AND OPERATIONS ARE ESSENTIAL	VS	SAFETY AND RELIABILITY ARE DISPOSABLE

FIGURE 7

SLANT OF BALANCE TOWARD BENEFITS

o RESULT:

- TAKING MORE RISK THAN IS DESIRABLE.
- PROBABILITY OF GREATER LOSSES THAN NECESSARY

o REASONS:

- THINK-POSITIVE SYNDROME (LATER)
- BENEFITS WITH HARD DATA VS. RISK WITH SOFT DATA (INCLUDING LOGIC)
- GRADUAL DEGRADATION FOLLOWING REACTION CAUSED BY SERIOUS ACCIDENT
- LESSONS FORGOTTEN
- MATERIAL AND POLITICAL PRESSURES
- UNCERTAINTIES LOST IN DECISION PROCESS. MICRO DECISIONS, ASSUMPTIONS, APPROXIMATIONS ETC.

FIGURE 5

WHY RISK DEPARTMENTS?

AGAINST

- o UNCERTAINTY DISCIPLINES OFTEN CONSIDERED A NAGGING INTERFERENCE.
- o DESIGN ENGINEERS CAN READILY UNDERSTAND AND LEARN PHILOSOPHY AND TECHNIQUES OF RISK TECHNOLOGIES.
- o DECISION MAKERS HAVE DONE WITHOUT RISK DATA OR ANALYSIS FOR CENTURIES.

FOR

- o PRIME INTEREST IN WORK ESSENTIAL FOR QUALITY.
- o CONFRONTATION

  BENEFIT VS RISK -

  IS ESSENTIAL ELEMENT OF DECISION

FIGURE 8

THINK-POSITIVE SYNDROME

EXPRESSIONS THAT DEFINE STATE OF MIND.

PREFERRED BENEFIT TYPE	RESISTED UNCERTAINTY TYPE
SAFETY	ACCIDENTS
RELIABILITY	FAILURES
QUALITY ASSURANCE	DEFECTS
TESTING	ANOMALIES
PROBABILITY OF WINNING	PROBABILITY OF LOSING
RELIABILITY .992	PROBABILITY OF FAILURE 8×10^{-3}

FIGURE 6

- DATA ON ANOMALIES AS IMPORTANT TO FUTURE AS MAJOR MISSION FAILURES.

- A WEALTH OF UNUSED STATISTICS IS AVAILABLE WHICH COULD BE USED WITH FMEA FOR REAL LIFE PROBABILITY PREDICTIONS.

FIGURE 11

CONCLUSION

1. SEPARATION OF BENEFIT & RISK MANAGEMENTS DESIRABLE BECAUSE OF:
   - --WORK INTEREST
   - --BENEFIT OF CONFRONTATION
2. MOST OF RISK TECHNOLOGY LAGS FAR BEHIND BENEFIT TECHNOLOGY IN:
   - --STATE OF DEVELOPMENT
   - --DATA BASE
   - --DEGREE OF ATTENTION BY MANAGEMENT
3. RELIABLE QUANTITATIVE DATA BASE WOULD MAKE MAJOR CHANGE IN UTILITY OF RISK
   - ---ANALYSIS OF OPERATIONAL ANOMALIES MIGHT PROVIDE NEEDED BASE
   - ---THEIR CAUSE AND WHERE THEY COULD HAVE BEEN CAUGHT
4. EXISTING LAG DOES NOT OF ITSELF JUSTIFY GREATER EFFORT
   - ---UTILITY TO DECISION-MAKING AN IMPORTANT CRITERION

FIGURE 12

WORK INTEREST

PRINCIPLE

Relatively Poor Performance Results in Areas of Secondary Interest When Mixed With Areas of Primary Interest

TABLE OF DEGREE OF INTEREST

● ● PRIMARY (1, 2)

▲ ▲ SECONDARY (1, 2)

RISK-RELATED GROUP	$	T	PERF. PARAM. KEY	PERF. PARAM. NON-KEY	UNCERTAINTY CONTROL: SAFETY	REL.	Q.A.	TEST	MAINT.
MGT (Decision)	● 1	● 1	● 1	▲ 2	▲ 1	▲ 2	▲ 2	▲ 1	▲ 2
DESIGN	● 2	● 2	● 1	● 1	▲ 2	▲ 2	▲ 2	● 2	▲ 2
SAFETY (RISK)	▲ 2	▲ 2	▲ 2	▲ 2	● 1	● 2	● 1	● 2	● 2
RELIABILITY (RISK)	▲ 2	▲ 2	● 2	● -	● -	● 1	▲ 2	● 1	▲ 1
MAINTENANCE (RISK)	▲ 2	▲ 2	● 2	● -	△ 2	● -	● -	● 2	● 1

FIGURE 9

NASA MO RV71-16181 5-18-71

CONFRONTATION

EFFECTIVE DECISIONMAKING REQUIRES:

- --- CONFRONTATION OF DIFFERENT POINTS OF VIEW
- --- INDEPENDENT THINKING
- --- ADEQUATE DATA & ANALYTICAL BASE
- COMMUNICATION CAPABILITY

FIGURE 10

9. IMPORTANT TO DEVELOP A SENSE OF THE DECISION VALUE OF BETTER BALANCE IN KNOWLEDGE OF BENEFIT-RISK RATIO BY:

--IMPROVED DATA BASE

--TRIALS & ANALYSIS

--STIMULATION OF PRIVATE CONTRACTORS

FIGURE 14

5. ARGUMENTS INDICATE GREATER RISK GENERALLY TAKEN THAN INTENDED.
6. NO CONTROVERSY THAT IMPROVEMENT IS POSSIBLE.
7. CONTROVERSY WHETHER IMPROVEMENT IS WORTH THE EFFORT (IS COST EFFECTIVE)

--MANY MANAGERS FEEL PRESENT CONDITION SATISFACTORY

--OTHERS DON'T (INCLUDING DEFENSE UNDERSECRETARY PACKARD)

--RECOGNITION OF NEED OF RISK ASSESSMENT IS RAPIDLY GROWING

8. DECISION MAKING:

--BENEFIT-RISK INFORMATION IS UNBALANCED

--CURRENT DECISION EFFICIENCY: NOT KNOWN

--EFFECT OF IMPROVEMENT OF RISK TECHNOLOGIES: NOT KNOWN

--LOSS INCURRED BY REDUCTION OF EFFORT IN UNCERTAINTY AREAS FOR SCHEDULE & COST: NOT KNOWN

FIGURE 13

AN OPINION

APPLICABLE TO PUBLIC AND PRIVATE SECTORS:

IF ONE DOES NOT INCLUDE THROUGHOUT A MAJOR PROJECT

--SYSTEMATIC UNCOVERING OF UNCERTAINTIES

--THOROUGH OFFICIAL ASSESSMENT OF RISK AT EACH MAJOR MILESTONE.

ONE LOSES ONE OF THE MOST IMPORTANT VALUES FOR THE FUTURE THE PROJECT CAN PROVIDE--

--DEVELOPING REAL-LIFE STATISTICAL DATA

--LEARNING HOW TO APPLY THEM TO DECISION MAKING.

FIGURE 15

SYSTEM SAFETY MANAGEMENT

A NEW DISCIPLINE

by

Mr. W. C. Pope

Chief
Division of Safety Management
Department of Interior

Presented at

NASA Government-Industry
System Safety Conference

May 26-28, 1971

A NEW DISCIPLINE

Credit safety engineers for a new systems theory to the complex aerospace industry. But credit also the safety managers for making their theory apply to the average industrial management activity.

A system is simply an assemblage of things and parts that go to make up a whole. Space engineers think of their complex and dangerous manufacture and manipulation of space products as a system. "All systems go" is their famous watchwork. The Defense Department has a set of general requirements for applying systems safety engineering principles to the life-cycle of weapons systems including the conceptual design, engineering, fabrication, testing, installation, checkout, operation, and disposal. (1)

This approach to optimal safety effectiveness has given the engineering side of loss prevention a "new look" that gives promise to an exciting future for the technical safety experts. The application of systems theory, however, is not limited to safety engineering and hardware. It can and does apply to any number of things, some of which are quite familiar to us. For example: a training system, a transportation system, the Federal Reserve System, the respiratory system, the solar system, the school system, and so on. THE THEORY OF SYSTEMS CAN BE APPLIED TO MANAGEMENT.

MANAGEMENT IS A SYSTEM

In a very practical sense, management itself is a system every bit as complex as any system of hardware. Organizations are man-made systems with many interrelated functional and subfunctional parts. Each is responsible to the other in the accomplishment of a common mission of the business. Each must work in harmony to accomplish mutual goals.

"The systems concept can be primarily a way of thinking about the job of managing" according to the authors of a textbook that presents management theory in a "systems" framework. (2) This concept of visualizing the system of management as a series of parts working together to contribute to a whole is very exciting for safety managers. This book along with the works of Gulick, Urwick, Blake, Likert, Drucker, McGreggor, and others is recommended reading for every safety manager desiring to adopt the systems approach to accident loss prevention.

MANAGEMENT CAN BE DEFICIENT

H. W. Heinrich, (3) a pioneer in the field of accident loss prevention, pointed out that accident events have (1) unsafe acts and/or personal factors and (2) unsafe conditions. What Heinrich did not discuss was the managerial failures or system breakdowns that are basic reasons for human errors and condition defects. These factors must be translated into broader areas of managerial responsibilities involving policies, organization, staffing, communication, coordination, decisionmaking, etc. at all levels of the corporate hierarchy. In this concept, safety managers must stop visualizing the problem only with the individual (supervisor or employee), step back, and see the problem from the systems point of view.

PERFORMANCE ERRORS CALLED "ACCIDENTS"

Accidents are only managerial excuses for operational errors that result from manager failures. This concept was introduced in 1962 by Dr. John J. Brownfain who said, "In science, if you know the cause of an event, that event is not an accident." (4) He went on to explain that "In everyday life, if we do not like the end result of this event, and at the same time want to escape personal responsibility for it, we are inclined to call it an accident."

Dr. Brownfain's observations are important in the system safety management approach to reducing operational errors called accidents. Few will disagree that causes of most accidents (events) are well documented. Thus, what safety managers are really doing for management is programming to eliminate performance failures that produce injury and property damage. Carrying this one step further, one can say that safety activities are directed more at managerial improvement than the reduction of personal suffering, although the end result does not change.

THE FUTURE OF SYSTEMS SAFETY MANAGEMENT

Systems safety management holds great promise as a new discipline for reducing

operating errors, conserving labor resources, avoiding operating costs due to mistakes, and for improving managerial techniques. The management approach to safety involves the process of business viz-a-viz the process of things. In this process we are concerned more with the interrelationships of all levels of management in relation to the prevention of loss rather than only with the line manager (supervisor).

After six years of practical application and research with the systems theory and safety management, it is my observation that:

* Improvement of a critical managerial weakness in the organizational system that contributes to operational errors can be equally as important as protecting a critical function of machinery. One cannot succeed very long without the other.
* The principle of redundancy (multiple channels of operation to reduce possibility of failure) can apply to the process of management as well as to a mechanical operation.
* Systems reliability can be as important to the excellence of management and its functional entities as to the successful engineering of hardware components.

In short, any operating error that is reported as an accident, can be examined for managerial failures as well as human errors and condition defects. The managerial deficiencies can be traced to the several management systems and, in turn, to their managerial subsystems. The isolation, quantification, and cost evaluation of these managerial concerns then become an important part of decision-making and eventual systems improvement.

MANAGEMENT MUST BE STUDIED

The successful use of the systems theory with the management of accident prevention programs as applied to corporate organizations requires the understanding by all line supervisors that most causes of accidents can be traced to staff support deficiencies. This information about causes and costs becomes a valuable management tool for self evaluation (upwards) and a means for controlling and planning with greater accuracy and efficiency.

From what has been said here, it should be fairly obvious that a safety professional who chooses the management direction of accident loss prevention must have a broad background of managerial expertise and experience beyond that of a line manager. The art of management is as important to the safety manager as the science of engineering is to the safety engineer. Some knowledge of both is an ideal situation.

Remember, in the field of management, interfunctional interest in safety begins with the establishment of common program goals between the functional systems. This simply means that the safety manager must know what the order functional manager is trying to do for the organization and then tie safety objectives to his objectives. For example, it would be extremely difficult to obtain management interest in problems concerning "falls-of-persons" from a personnel officer - or even a property officer. On the other hand, tell personnel it has a "training" deficiency that produced over 1,000 employee errors resulting in falls, or tell a property officer that design failures are causing $200,000 of waste annually, need any more be said? In each case, the managerial weakness is degrading the expected output of the system in an area of concern that cannot be corrected by the safety manager.

Others interested in loss control (error-free-performance) will show concern if that loss is presented in a way that relates to failures in their fuctional missions or to the ability to operate and manage for profit.

If you want management's attention to safety problems, then speak management's language and be sensitive to managerial concerns. Learn all you can about each function and subfunction of your business in the same way that an engineer is expected to know about machinery he deals with. This will enable you to make serious inroads to their decision-making process. ABOVE ALL--CONSTRUCT YOUR SAFETY SERVICES TO THEIR ORGANIZATIONAL NEEDS NOT JUST TO THE REQUIREMENTS OF AN INDIVIDUAL.

CONSTRUCT AN INTRA-MANAGEMENT INFORMATION SYSTEM

Control is the basic feature to the systems theory. You can solve a problem if you don't

have the facts about it. This means that a safety management information system is basic to managerial improvement through loss prevention. This communication upward through the levels of management must be responsive to managerial needs. Use a computer to collect and store accident data related to management systems. Used correctly, safety managers will not have to beg for top management support. Functional managers at all levels will seek safety support.

No system can exist without communication. The first task in establishing a report network is to develop a source document (accident report) that allows the line manager to identify systems failures. (5) He reports them, as he sees them, in a manner that can be put into a computer. The computer can be called upon to feedback data for periodic analysis in meaningful terms (English language). This analysis with supporting facts is then given to the line managers for direct action to staff managers for systems improvements.

CONCLUSION

In summary, it would be a serious mistake to think that the theory of systems and safety applies only to hardware. Engineering or technical knowhow is not the prime requisite for all safety problems. Expertise in safety management requires a basic understanding of human resource management rather than scientific understanding of machines.

To make the concept operational, safety managers must consider always the social benefits of employees--their needs, motivations, and asperations more as groups than as individuals. There is a great need for understanding of group behavior and manager relationships and the safety manager may make a real contribution to errorfree performance by the realization of this need.

"Some loss control programs are now showing refreshing signs of objectivity" says Robert LeClerg, Assistant Chief, Administrative Operations Division, National Oceanic & Atmospheric Administration, U.S. Department of Commerce, "They share responsibility for finding and identifying all accident losses. They collect causal data in usable form instead of simply keeping score. They bridge the Communications gap by addressing dollars and manhours lost instead of percentage of rates. This momentum is well timed to reinforce the new emphasis on "ZEROING-IN" on problems. But, before we pull the trigger, let's examine the target. Our purpose must be to give effective direction to the control of all accidental losses, not to play one more hand of the same tired game". (6)

REFERENCE

(1) Refer to "Systems Safety Engineering of Systems and associated Subsystems and Equipment, General Requirements for MIL-STD 882" June 6, 1966, for all departments and agencies of the Department of Defense.

*Reproduced by the National Safety News, National Safety Council, May 1971

(2) Johnson, R. A., Kast, F. E., and Rosenzweig, J. E., "The Theory and Management of Systems, "McGraw-Hill Book Co., New York, 1967, p. 3

(3) Heinrich, H. W., "Industrial Accident Prevention," McGraw Hill Book Co., New York, 4th ed. 1959

(4) Brownfain, J. J., Ph.D., "When Is An Accident Not An Accident?", JOURNAL of the American Society of Safety Engineers, Park Rige, Ill., 1962, p. 19

(5) Pope, W.C., and Nicloai, E.R., "In Case of Accident - Call the Computer", Personnel Pamphlet No. 23, U.S. Department of the Interior 1970

(6) LeClerg, R.E., "A Revolution and How to Treat It", FOCUS - Journal of the National Safety Management Society - Environmental Control & SAFETY MANAGEMENT, A.M. Best Co., March 1971 p. 37

N72-25964

DATA REQUIREMENTS ANALYSIS IN SUPPORT OF SYSTEM SAFETY

by

Mr. Irving Pinkel

Chief
Information Services
and
Publications Branch

Aerospace Safety Research
and
Data Institute
NASA-Lewis Research Center

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

Those friends of George Mandel who are wondering why it is that I am here in his place, I am happy to report that he is recovering nicely from a heart attack.

On the matter of the Aerospace Safety Research and Data Institute, about three or four years ago, after the Apollo fire, NASA realized that its safety organization could use a center where safety information accumulates and is validated and interpreted for use by the Aerospace Industry. Our group was set up in the Cleveland laboratory to serve all of NASA and the Aerospace Industry. Three years ago I was a lone member of this group and I spoke to this conference about our hopes. Now I am here to report how we have proceeded, what our points of view are, and where we stand at this time.

Let's review for a minute and take a look at our objectives. First, to support NASA and its contractors with technical information and consulting or safety problems. To identify areas where safety problems exist or where voids in technology exist, and to initiate research programs both in-house and under contract to fill these voids; to prepare state-of-the-art summaries and other publications of use in our area. The key to all this is to establish and operate a safety data bank.

It is my purpose today to go through this quickly to give you an idea of our thinking and where we stand. I might add, as an overall remark, the emphasis we have given in our efforts is to keep the user of the information in mind. That user isn't necessarily a safety specialist as you are, but can be any one of the engineers in the total system of engineering support. There are decisions being made at all levels. Many of our users are competent engineers who are being called on to make decisions involving technical information for which they have poor background.

In order to maintain contact with the user population so that we do a useful job, we stay in detailed contact with the entire industry and all institutional centers of NASA where problems are apt to arise. We also have membership on a host of committees. Obviously the space shuttle is prime to NASA's interest at this time and I might add that in setting up this data bank we try our best to do the work in those areas of immediate interest to NASA and then broaden our interest as time allows. Space Shuttle is being controlled at this stage by a variety of committees within NASA and we have panel membership on each of these committees. We worry about cryogenics and low temperatures systems because we deal a great deal in propellants which are liquified gases, and we have membership in the Compressed Gas Association where much of this work is done. I won't detail all of these things but point out that in addition to all else we deal with assorted NASA committees dealing with space-borne radioactive materials. If you are wondering how it is that NASA deals in radioactive materials for space, I will remind you that the largest space station which will orbit the earth will carry electric producing systems which will not use the sun as a source of heat but either a nuclear reactor or radioisotopes. This is a real concern to us at this time. The final committee we serve on is NASA's Spacecraft Fire Hazard Steering Committee which I chair. This grew out of NASA's concern for fire problems on spacecraft, particularly manned spacecraft.

The question is, What is Safety Information? We had to ask ourselves, we are going to collect information, but what? What is it? Is it that body of information that has a safety label attached to it in someway? Well yes, it is that. But is it something else as well? Here is what we feel constitutes the boundaries of safety information and I am sure this is an inadequate detail of these boundaries. First, safety information is a body of technical matter drawn together from various disciplines in support of a safety problem. This information is often indistinguishable from engineering, scientific or medical information. In a sense, what we are saying is this, that safety information can be drawn from any part of the technical and scientific literature and we have to be prepared to do just that. Safety information is also information on hazard management techniques, and where equipment is involved, the associated equipment. It deals in failure advisories, accidents, reports, and then the legal aspects of safety, codes and standards.

Now, where we are dealing with a user-oriented system, the user generally comes to a safety problem with certain categories of questions in his mind. He would like for example to recognize when hazards exist, and understand how he can detect the build-up of a hazardous condition. And so we like to organize our information that way. Or he would like to

understand how to reduce the probability of a failure or an accident. So we organize our information this way as well. He would like to be able to assess the consequences of a failure. Oddly enough, when we look at the literature for assessing the consequences of a failure we don't go to the safety literature, we go to the anti-safety literature. We look to the demolition expert and say, "what do you know about what would happen if we had an explosion". He would like to be able to reduce the consequences of a failure and he would like to have the information so structured that when he comes with this question in mind he can find that kind of information.

Then there are certain scientific and engineering fundamentals he has to have in order to apply what information exists. We feel that here is a kep weakness in the communication of safety literature, information from the literature, and that is the interpretation of what the literature tells you. We feel that in many areas, we, the Aerospace Safety Research and Data Institute, shall have to prepare documents which show how the existing information in the literature is interpreted in terms of real problems. We haven't begun this process yet except in a very limited way. It is a difficult thing to do, but I think it is a vital step. And we also, since the legal aspects of safety are so important, have to make our engineer who is dabbling in a safety problem aware that there are certain legal aspects to the safety problem.

When we took a look at the existing information in safety and decided to create a safety data bank, we were first faced with what shall go in the bank? We are proposing to have a largely computerized bank and the first thing that hit me forcibly in this whole business was the fact that if you use a computer as a bank, as a place in which to store information, you discover how enormously, enormously costly it is to do a proper job of putting information into a computer. We said we have to be careful what goes in, not only from the standpoint of cost, but from the standpoint of credibility. Can the people get information out of our system and depend on it? They are surely going to use this as an authority for the actions they take and if we give them the wrong information or poor information, it is our responsibility. Also, we looked at the quality of safety information. Most of you are old pros at this and I think you'll want to disagree with what I am going to say next.

In the safety information that we reviewed, we often found that important portions of the safety information are misapplied laboratory data. Data that was gathered not with a safety problem in mind but simply a study of a discipline, and somebody is using that information improperly in a safety document. Safety reports often deal in opinions masquerading as fact and this is all too often the case. I think many of you understand this. A large body of literature exists in some fields and little or none in others, and sharply focused information is difficult to find for both reasons. There are times when you query an information system about a certain aspect of a safety problem, you get snowed with 2,000 documents. That is as good as giving you nothing unless you have enough discretion in the field and are inquiring enough to pick that which is useful from that which isn't.

Much of the literature contains incremental contributions and a large mass of reports must be reviewed for answers to the safety questions. This tells us that somewhere in our system we have to boil down the information into review and summary reports and let that be the input to our system and cut out the chaff of a large number of incremental reports. And too, a point I alluded on before, information is couched in scientific terms which are unfamiliar to engineers. In other words, the information isn't user-oriented. If you want to touch on this at all, give an engineer a man-machine problem, the business of integrating man into a machine system, and let him look at the data the psychologists put out and try to make some sense of it for himself. I'm not saying that psychologist's data is no good, but the psychologist's data is so couched in jargon that the engineer is hopefully confused.

The present retrieval systems often lose the relevant information and cite many irrelevant references. When this happens, obviously there is a degradation in the service being provided.

Here is what we said the components of a safety data bank system ought to be.

First, we should use a computer, should be document references. These should have an appropriate abstract so that the person looking at a document reference doesn't have to go by the title. Authors of reports are notoriously

poor in titling their own reports so we prefer to have an abstract which helps a little. In the work which we are going to be doing, which we ask people to review literature in specialized fields, we ask the reviewer who is an expert in the field to write his own abstract in addition to the author's abstract, if he thinks the author's abstract is misleading. Computer information should have references to other repositories that specialize in information, and I want to bring up the point that we don't think we are the only safety data bank in existence. We know there are many. We hope to be complementary with them; not to overlap them, and in no case to totally absorb them unless it's worthwhile to do that. We do have to know where the other information resides and to have the computer point it out as an answer to a query on information requests. It has to be able to store systematic accumulations of safety data and what I mean by systematic accumulations is this. Much of the information that a safety engineer, or person involved with safety problems needs to use, have never been published. It has been garnered from research, completed in private places and these are available to us as curve and graphs etc. plots, formulas -- we have to be able to include that in our system so these come out. We can't rely entirely on documents. We then need a list of specialists in safety and safety-related fields and this goes back to our role of consulting. We ourselves don't feel that we are capable in every field to give consulting. This would be ridiculous for a group of about 16 technical people, and we couldn't hope to cover all fields. What we hope to do in providing consultation is to find an appropriate person somewhere who can serve that role, but we can't.

We don't intend to supplement the standard reference library with on-shelf references. There is no sense in sticking the normal materials of a good library in a computer. That's on the shelf and the standard library techniques work very well. We hope to microfilm all the information that is referred to in our computer-stored information so that if the person wants the reference we can slip him microfilm. We next hope to set up a Safety Information Analysis Center for consolidating this act of boiling things down and having only a few reports in the place of many; validating, in other words getting rid of the junk that isn't correct; and updating, getting rid of old stuff and making sure you're getting the latest in safety information and then prepare safety reports and advisories, much of which would be done under contract.

Now where are we in this matter of establishing the bank? First, our basic computer components have been acquired for the Lewis Center and they are being up-graded which makes me unfortunately say to you that we can't give you red-hot service quite yet because this up-grading step makes the computer unavailable to us for long periods of time. We have now completed the computer programming to give us a very flexible storage and retrieval system for information. First of all we give random access to documents and data citations in the computer storage, in other words very speedy retrieval. We can reach into any part of this storage immediately and pull out the reference without having to spin all tapes through a monitor to pick up the information we are looking for. This reaches in and pulls it out in a fraction of a second. We can fix the retrieval of information by author, by content, in which we use an elaborate system of key words so that you can get sharply focused information, by document origin and number, and I might add by the contractor or other Agency that did the work, by the program name that created the work and so on. There are many ways in which we can find documents under this system. We believe in continuous key-word Thesaurus development. These key words are the descriptives that describe the contents of a document. We know that as documents appear, any fixed Thesaurus will not cover the contents of an evergrowing field, and so the Thesaurus that we are developing can continue to grow with the literature as it comes in and we can always have an up-dated Thesaurus. When a searcher comes to the computer and says I want to find something, what word shall I use. The computer gives him the very latest list of words. The system is very flexible in that if we feel that having enlarged the Thesaurus and the descriptive terms that we allowed ourselves to use, we did an inadequate job of the existing citations in our files, we can go through and change the key words attached to that citation. In the end we hope to be free of any business of a Thesaurus and use free language for characterizing citations. In other words you have a freedom from the constraint of using

specialized terms. This is one of the difficulties of finding information in a computerized system. The systems, if they are limited to a Thesaurus, have a rather strange number of constraints.

Let me give you an example of this: Suppose you were interested in cats. And in particular, since you are domesticated, you want a domesticated cat, you want a house cat and you want information on house cats. There are some retrieval systems that would say, "Okay, you can use the word house and you can use the word cat. Because the C in cat comes before H in house it will go into the computer with the word with the C first so it goes into the computer, not as house cat but as cat house. Now who would think of looking for house cats under that. You can do a lot of games with this of course. Try venetian blinds for example. This is true, some systems are this way and give the searcher quite a game to play to try to find the information that exists. We hope to break this block.

We will include a file of document abstracts and reviewers comments in which the reviewer will say the report is pretty good for this area of work but don't believe the title, it just doesn't have very much information in another area or, this is old stuff and it's wrong in this respect. We hope the reviewers comments will be tagged to most of these citations. As I said before, we would have a method for accumulating incremental data in terms of tables and formulas etc. and also the computer has devised within it a means for assisting the searcher in going through the strategy of the search. It keeps assisting him with clues and if he doesn't know what to do next, he asks the computer, "What next?" and the computer tells him.

Here is a view of what we are trying to do now. First of all we find that there are some excellent safety information files. Many of them are computerized, some are not, many of them have this so-called interactive--let me say it this way--we are more or less unique in having this easy interactive scheme of search and retrieval that many do not and where it's justified to absorb a given file or information on safety so we can have this nice access with our computer, we do this. In particular, an excellent file of safety information, which has already been put into our system is a file of about 35-36,000 documents in the nuclear safety field. The files of the Cryogenic Engineering Center and the National Bureau of Standards has already been placed into our system. The FAA Aviation Safety files, we are negotiating on. Recall we said that a complete information system would also include component failure rate files and here is the key word--IDEP--it is an information exchange program amongst the various segments of the Government. It deals with failure rates in the testing of components for aerospace devices--airplanes, spacecraft. By putting this file, which exists on paper, into our computer we can maintain an up-to-date record of all failure rate studies going on, that have gone in the past and those which are current. This will keep some branch of the Government from repeating a failure rate study on a piece of equipment which is already in progress by another Agency. You'll see a sample of the kind of print out this system gives.

Within NASA, following the 204 fire four years ago and then the Apollo 13 accident, both involving oxygen, and other oxygen accidents within NASA, we undertook a complicated and rather involved study of material compatibility with oxygen. This file is going into our computer so that one can find information more readily than the turning of pages in a book, which becomes very difficult.

Here is some safety information that we are asking others to gather with our support and our help. Oxygen System Safety, this grows out of the Apollo 13 accident, in which we are collecting meaningful literature and data and then we are collecting the practices of others in design and operation of oxygen systems. We are trying to put together the fire technology as it applies largely to spacecraft and aircraft and ground test facilities in support of development of either of these. The National Bureau of Standards has a contract with us to do this. They have a fire safety technology group who are charged by Congress to conduct work in this area. This portion of it is a cooperative effort with NASA now.

Human Factors, with emphasis on flight vehicles and especially the space shuttle. This study is going forward under the guidance of the Human Factors people at our Ames

laboratory in California and it is to be a major effort. This Nuclear Isotope safety I mentioned earlier has to do with on-board nuclear materials. The business of non-destructive testing and diagnostic techniques with structures on machines safety codes and operating practices for aircraft, fracture mechanics data for structural alloys with special emphasis on low temperature applications of metals and let me cue you in here. NASA has found that every time it took on the use of a high strength material, particularly those which retain their high strength at low temperature, it found it had problems in fracture mechanics--the two ran together. When you try to grab the advantage of a red-hot material that had a high strength to weight ratio and good toughness at low temperatures particularly it had a fracture mechanic problem. The thing wanted to crack easily, which appears to be a contradiction of terms, but this is the way it works. Mathematical techniques in safety analysis, that is only beginning for us.

In an effort to organize our information so that the user can find his problem, we did this. We said, the user comes with certain questions in mind, very often he is concerned with the causes for failure in his systems and we are taking as our illustration this cryogenics fluid safety grid and a means for characterizing the information that exists in a given area and in this area on cryogenic fluid safety, what are the causes of failure? and we say the causes of failure under what conditions. When you are transporting, where you are storing, when you are handling the fluids in systems. These are the blocks which represents an intersection between this term, transportation storage or system handling, and failure causes. Each of these blocks constitutes a range of problems of interest and these then are the categories we create, this range of problems of interest, and place them in this chart so that a person with this problem on his mind under these conditions sees what has been done here. Not only do we do this but all these words that are descriptive terms for describing the literature that exists in this area will appear in this block. That was a simplified view of things--I think you can read the rest and appreciate its relevance to some of the remarks I made before. This is a simplified view only for our purposes here. If I were to show you a true chart, the one that developed for the fire problem, I think you can appreciate that it is a fairly involved chart. The hope that is on perusal by the user, the person who has a problem in mind and then comes to our system and says where can I find information and we give him this, he gets a first clue into how to interrogate the system to find his information. What words does he use to the computer to say give me information along these lines and the computer will begin to formulate a form.

This chart is also used by the people who input the information into the system and any key words that they develop to describe the contents of the documents they review go into those blocks so that the user, the guy searching sees the words that the inputter created to describe the information that exists there.

With regard to the IDEP record, this is the business of putting into the computer a record of the failure rates for equipment under test. The purpose of our computer handling of this is to tell a searcher where he finds the record on the piece of equipment he is concerned for. The address, because the IDEP system provides microfilms of all tests and there is where the information he wants resides. The question is, where is it. In all of the tapes that exist, all of the microfilms, in other words, he is looking for this address, the microfilm address code number. Once he gets that code number, he knows how to spin his microfilm to find out where the information exists. Now he can find the component he is interested in in a variety of ways. He knows the accession number, (I won't try to describe these terms in two much detail, I don't have time) the manufacturer, say the company, of the equipment, the date it was made or the date of the test, or the government part number or a description of the part. May be it is a relay, the contact rating in this area etc. He feeds this to the machine. The machine then prints out a page that looks like this and he can check and see whether this is truly the piece he wants, and is this the correct part number if he has the part number of the Vendor's part and so he says, Yes that is the right one and he knows where to search in the microfilm.

From time to time NASA puts out alerts on parts and this we hope to have in the

machine and the key issue here on the alert, not worrying about anything else is this, that people have in the machine a system of alert. If somebody is concerned about what the latest alerts are, he simply queries the computer from a remote station, a console remote from our system, by telephone lines and asks what is the latest alert. He gets a statement which says failure analysis conforms something about a part and the trouble with the seal, etc. and he can identify what the alert is trying to tell him.

With regard to other data centers, we have identified about 150 data centers which we think are useful in our business. There are probably more. We hope to have them within our computer and we ask for certain information and say what data centers would have information on particular things. The computer would print give a print out; which would give them the name of the information center, say Electronics Properties Information Center, and then what do they cover in that center. If you are concerned for liquid metals and hazards associated with these, this is the kind of coverage the liquid metals information center would give you. Not only do you get this, you get information on first, the name of the Center, where it is, how you get information from them, do you call them up, do you send them a letter, do you have a fee to pay, etc. We hope that our Information Center will be one of a network. There are many good ones that have capabilities like ours and we hope that we can tuck them all together in one network so that when you query the system you query everybodies data base. We are trying to make our system consistent with this point of view. If you want to be part of this system and you want to query the information that we have, do you have to call us. I hope not. We would be available for any calls or for any letters in inquiry. What do you have on some kind of problem but we hope that those who are principal users of safety information will have their own console substations which are reasonably cheap. A $5,000 or $6,000 investment gives you such a station. With this tie in, you dial the telephone, FTS or any other voice communication line will put in communication with our computer and gives you the opportunity to access it for information only. This doesn't give you the opportunity to change the contents, only to get the contents out.

It is made of three major components. First a TV screen on which the print-out of the computer is placed and gives you all the information regarding the document you are looking for; a keyboard for instructing the computer on what you want next; and if you see something on the TV screen that you like and want to preserve after making a search, you hit a button on the keyboard and a print-out, permanent record hard copy appears here. These are the three components. For an investment of $5,000 to $6,000, you get them all.

We hope that when our system is rich enough to justify others having remote stations. Our hope is that we can handle many queries, 40 people on the line simultaneously.

That then concludes my description of the work we are doing.

Thank you.

REFLECTIONS ON SYSTEM SAFETY

AND

THE LAW

Mr. Daniel F. Hayes, Sr.
Assistant
NASA Director of Safety

NASA Headquarters
Washington, D.C.

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

HOW SAFE IS SAFE?

The question "How safe is safe?" will be frequently directed to those who work at preventing accidents. The question will often take these forms: How far do we have to go with these precautions? how much money or effort shall we spend to prevent accidents? do we need "redundancy," "back-up," "guards," "fail-safe," "emergency procedures," "more training?" if we provide backup for an operation, shall we backup the backup? If we do, how much safer is it? If we spend money to reduce the hazards all the way, is it worth it? Is the benefit worth the risk? This last question has become a most serious one for business men today in the light of increasing awareness of the public and attending claims consciousness. While still not taken as a national policy, it is becoming more and more recognized that "accidents can be prevented." And so--how much prevention?

We safety managers have a notion that we know what is safe. No doubt! Experience teaches us to know better than some others what is safer, and only perhaps what is unsafe. But "safe" and "unsafe" are general, abstract, unquantified, relative terms. Here-to-fore we have been successful only to the extent that we have given more attention to eliminating or controlling conditions from which accidents can arise which are discernible to a trained eye.

The unconscious desire of specialists is to prevent change in their specialty--(A quotable quote from one of the cases)--"To a specialist "change" means unlearning a section of knowledge, a painful process!"

With the development of additional attention and emphasis on safety and the greater urgency technologically, socially and politically, we are refining the search to prevent accidents with the more diligent application of engineering methods and the stricter use of logic and of computer selected information. Thus conditions that were formally called "accident causes," are found out or discovered, and anticipated, and the potential for loss eliminated, controlled, or otherwise negated. We find that many so-called accident causes were not unforeseeable and unpredictable! We didn't search with sufficient diligence! Thus system safety analyses become, not panaceas, but only aids to anticipating what was formerly unanticipated. The probabilities have been qualified and quantified. The result of these efforts permitted us to send men to the moon and bring them back safely. They can be used in many other applications with similar success.

THE ANSWER IS LAW

But this search still does not answer the question fully--how safe is safe? It only tells us that asking "what if?" often enough and providing the answers will make our hardware, process or management safer. In fact, to be able to go all the way, will require more than human clairvoyance. I submit that in any given situation the question of whether this process has been followed to an adequate degree will usually be explored in a court of law.

Safety is a state of being free from or the absence of danger. Danger is a positive word and means that there is a potential for harm or loss. (Incidentially, the word for "safe" in Russian is the equivalent in English of "danger" (oposnosti) plus the prefix "without" (bez) which makes it "safe" i.e., without danger.) Harm is damage or hurt. And, unless the hurt is to the perpetrator himself, there can be a claim for negligence. When negligence is alleged in a court action to be the cause of the damage, we are all set for a determination of "how safe is safe" because the law will want to know among other things "How diligently did the responsible person look for the causes of harm and what did he do about them."

Throughout the cases of negligence, definitions and court determinations are generally consistent. In general "negligence is an act or omission in violation of duty to exercise ordinary care by reason of which injury to person or property occurs."*

Courts always imply that the negligence or failure to do or not do was what a reasonable or prudent person would do or would not do under the circumstances.

PRUDENT PERSONS WILL ANALYSE

It is my purpose to advance the idea that in some circumstances "what a reasonable or prudent person would have done under similar

*Sec. 32, 38 AM. Jurs. P643.

circumstances" will be to make a systems analysis. So far I have been unable to find adjudicated cases where this has happened, though I've been told it has.

If there are any, they are rare, so far. However, one does not have to stretch the imagination to realize that under many circumstances, now developing in products safety, technical operations, complex machinery, aircraft, pollution and other modern situations, negligence will consist "in" not having looked as systematically as one could have. "The policy of the law has relegated the determination of such questions to the jury (i.e., was he a reasonably prudent man?), under proper instruction from the court." When products and processes become too complex for a jury to understand or too technical for a judge to comprehend, some other means than rhetoric may be needed. What is "ordinary care" may be quite difficult to explain. The search for negligence has already been extended all the way back to defects in design. Such cases put a strain on laymen and technical terms before the judge. What better way in a technical situation to demonstrate to a jury how diligently one has sought out and eliminated those circumstances which could cause actionable harm or loss? Particularly is this so when the expression "the analysis applies throughout the life cycle of the system" is honestly applied.

From a case in the books--"A reasonably prudent man will neither neglect what he can foresee nor waste his anxiety on events that are barely possible..." [What is barely possible has only been occasionally quantified in legal thinking. Not so, in a system analyses. In some analyses, the "barely possible" is actually put into numbered probabilities.] Continuing the quotation--"but he, the reasonable man, will order his precautions by the measure of what appears likely in the known course of things, whether the particular act or acts charged in the petition were performed or omitted and whether the performance or omission of some of them was a breach of legal duty."*

This, in legal terms, describes what one does in a logic analysis!

Having made an analysis the step by step documentation required in practically every Safety Analysis Report, Operations Readiness Review, Fault Tree Analysis, Failure Mode and Effects Analysis, etc., provides recorded proof that one was diligent, not negligent.

The day may be here already, considering the advances in technical knowledge and techniques for retrieval of hazard information and accident experience, that a man or person (corporation) may be considered negligent if he has not used a system analysis in the degisn of a product to offer to the public.

If this theory is to be of value, the question of admissibility of such proof will have to be considered. This will be touched later.

THE LAW CHANGES

Argument for use of system safety techniques as a legal instrument is supported by several considerations. These techniques are certainly new tools. They have accompanied the growth of recent technologies--atomic energy, aircraft, space. But law and lawyers use new tools, too. The needs of a changing society will be reflected in the decisions in the courts. This growth and change in the law is most interestingly dealt with in a book titled "How High is Up" by Loth & Ernst.* They trace, in some of those fields, the manner in which law has adapted itself to modern new problems beginning with the legal concept "caveat emptor" i.e., "buyer beware." They show how this concept was changed in a few years, by reason of the "Cardozo Revolution," to a 180^{0} attitude and is now "caveat vendor", (seller beware).

They, Loth & Ernst, show that concepts of liability in aviation brought about vast changes in the law regarding ownership of land and air, and the effects on the posture of society in respect to noise, vibration, comfort, right of way, personal injury.

In McPherson v. Buick, 1916 Judge Cardozo said, "on the basis that science perfected previously undreamed of safeguards against inanimate objects and also much more damaging objects the vendor has a responsibility and a liability if he was placing a dangerous object on the market." Later interpretations placed liability on aircraft manufacturers, based on

*Sec. 38-28 Am Jurs. P645

*Bobbs-Merrill Co., Inc., NYC, LIB CONG. 64: 15-665

the lack of reasonable care in the design and control of quality. I dare to predict that the law will recognize and use, logic techniques, technological advances in the storage of accident information, system safety analyses, the tests and measurements and requirements for documentation that the space industry has developed.

It is not unreasonable to expect that in the field of negligence, warranty, breach of contract and rules of evidence, the law will adapt to more systematic assistance in seeking out the truth in appropriate cases, by the very means used to assure safe hardware.

AS EVIDENCE

The books say "Proof which is addressed directly to the sense of the court or jury without interposing the testimony of witnesses--is the most convincing " The presentation of charts, diagrams or tables which makeup the analysis would, no doubt require the engineer or persons qualified to be present. Diagrams or charts showing the basic assumptions of steps and stating the manner in which a system safety analysis was made and the controls which were applied will probably be allowed as evidence. The witnesses would be required to be authenticated by the presiding judge.

Let us look at another aspect of system safety and evidence. How well would the documentation required a system safety analysis serve the lawyers?

"In general where a map, or a drawing is offered as embodying in itself, the knowledge of the witness to which he, in this form deposes, the verifying witness must be shown to have personal knowledge of the facts so as to qualify him to testify to their correct representations. . ." It is my feeling that the step-by-step documentation not only provides the witness with a most potent method of recall, but it also demonstrates that nothing within the power of the intellect has been overlooked in the search for safety, and that there was diligence.

TESTS

"The courts, though they do not favor experiments and tests by the jury itself, now very generally permit relevant experiments, demonstrations or tests by others in court or permit evidence of experiments performed out of court. . ." This would seem to say that tests made as part of a hazards analyses, where the probability (or improbability) of failure is to be demonstrated, would surely be admissible. Similarly, tests which frequently became part of a system analysis will probably be admissible.

RISK VERSUS BENEFIT

The queries "What is safe?" or "How unsafe is unsafe?" are also tied into the construction which may be put on the concept of "benefit versus risk."

Ernst in "How High is Up" says "So law must always strike a balance between risk and recklessness." He mentioned this (he said) because it struck him as exceptionally plain in considering atomic energy." But use of atomic energy is not the only situation where this question is being posed. We see it frequently, for instance, with respect to environmental pollution, now considered as a great risk. Here it would seem that the law, when faced with this dilemma, risk vs benefit, will be greatly aided when the engineer or scientist applies his informed logic before hand, in respect to what the risk is, that is to be balanced. So it is possible that the precise quantification of hazards by technical analysis may more clearly help to determine the values of risk and benefit for the law as well as for the engineer.

ACCIDENTS FEED THE LAW

In the field of atomic energy there have been relatively few successful litigated claims for damage. In fact, few accidents. I can speak here with some knowledge, since I wrote the first complete repertoire of all accidents involving nuclear energy, which is now an Atomic Energy Commission biannual report. At the time there was no collected history, and I was somewhat surprised that the report sold over 7,000 copies at the Government Printing Office. The whole application of a new energy source and its integration into society is an instance where the lack of accidents, due to the rigid requirements written into the law relating to its use, the extreme caution exercised in the

manufacture and control of these hazardous materials and the experience with other kinds of energy deprived the courts of precendent on which to base decisions. (This further supports the thesis that until there is loss or damage we have no measure of what is safe or unsafe.) It will be interesting in the future as to what weight will be given by the courts to the extreme care exercised in the control of this hazard including the Safety Analysis Review system of analysis.

When accidents do not occur, both plantiff and defendent are left without a good measure of the relationship of benefit and risk. For the question of excessive risk is going to depend on what the courts decide is excessive, that is, whether the controls were or were not what a reasonable man would have done--and whether even so, the public benefit prevails.

STRICT LIABILITY

In certain situations a product or process is held to be hazardous without further proof to the contrary. This raises a speculation. In the doctrine of strict or absolute liability the person who puts a hazardous product on the market without performing certain actions such as warnings and specific instruction to the buyer will be considered negligent per se. However, it would seem the absolute liability might someday be successfully fought off and the trend turned, shifting the liability back from the vendor and giving him a chance to plead benefit to the public and the absence of unevaluated hazard. The law makes its changes in small steps. The application of new methods of engineering analysis are also steps usually in the direction of greater precision and sounder logic and safety. Perhaps these technical steps toward greater perfection will be the occasion for new legal approaches. It may be possible to avoid throwing up one's hands and saying "This machine is too dangerous to allow man to use it." It was only a few years ago that the possibility of atomic energy for power was abhored--today there are many nuclear power plants on the line in spite of the fears of the public and the experience is good.

When I became interested in the relationship between system safety analyses and the law, I had not looked at a law book in many years. Consequently, changes were very apparent to me, and the possibilities of changing from absolute liability back to a defensive position by reason of an engineering procedure that looks at, identifies and eliminates hazards would seem quite real. "There are few constants in the law but continued change. . ."*

Given a hypothesis or doctrine of strict liability there must also be a corrollary that says "you may do something or offer a product in the first place." That is, you are not prohibited to do so, but if you do so, the law says you must be prepared to be liable for it. In other words you are deprived of defenses normally available as to being a reasonable man. I submit again, subject to argument of course, that here is an ideal situation for use of logical analysis of risk. By using (and perhaps by usage) a system safety analyses will allow you and the court to arrive at a more precise idea of the true hazard, correct and control them and provide proof that the previous strict liability is not to be assumed.

APPLIED TO THE ENVIRONMENT

The National Environmental Policy Act of 1969, P.L. 91-190, 1970 imposes requirements on all Government agencies to interpret and administer their policies, regulations and public laws in accordance with the policies set forth in the Act. Those policies relate to conservation and use of the environment, and assuring safe, healthy, productive, esthetic and culturally pleasing surroundings, and other purposes. These requirements will fall on industry to an increasing degree.

To accomplish these purposes the Congress states under Sec. 102 of the Act that the agencies shall--

"(A) utilize a systematic, interdisciplinary approach which will insure the integrated use of the natural and social sciences and the environmental design arts in planning and in decision making which may have an impact on man's environment;

(B) identify and develop methods and procedures, in consultation with the Council on Environmental Quality established by Title II of this Act, which will insure that presently unquantified environmental amenities and

*Effective Research - Price & Bittner, 1953, Prentice-Hall, NYC

values may be given appropriate consideration in decision making along with economic and technical considerations;

(C) include in every recommendation or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment, a detailed statement by the responsible official on--

(i) the environmental impact of the proposed action,

(ii) any adverse environmental effects which cannot be avoided should the proposal be implemented,

(iii) alternatives to the proposed action,

(iv) the relationship between local short-term uses of man's environment and the maintenance and enhancement of long-term productivity, and

(v) any irreversible and irretrievable commitments of resources which should be involved in the proposed action should it be implemented."

It is the five specifics under (C) that deserve our attention when pursuing the subject of the title of this paper.

As written, those requirements paraphrase quite suitably the basis for a systems analysis. The objective of a systems safety analysis is to avoid an undesired event, in this case one which will pollute the environment. In a systems analysis of a piece of hardware this event is equivalent to a failure resulting in damage or loss of a mission.

The methods available such as Fault Tree, FM & Effects, Gross Hazards Analysis could be used to identify the events which will bring the pollution about.

The selection of available alternatives to the proposed action as required in this law will become possible when, in the analysis they are pin pointed.

The commonly used term in the analyses of space systems is "trade off." It accurately described item (IV) relationship above.

And finally item (V) is a statement of the residual hazards and the requirement on which management decisions must be made.

The usual hard requirement in a system analysis is that each step is documented, and that the whole analysis provides for sound management decisions.

The administration of the requirements of the Environmental Act place an added burden on almost every project or activity of any importance and--it would seem that system analysis would provide a simple and effective procedure to assure that a given project meets the intent of the law.

Summary

The final answer to the question of safeness is stated by the courts. What is "safe" changes with experience.

As technology advances new tools are developed. The new system safety analyses (methods) are such tools.

The law and lawyers use new tools.

The needs of society will be reflected in decisions of the courts.

These decisions change the law step by step.

It is not unreasonable to expect that the law eventually adapts its decisions as to what is or is not safe to the real world, and better engineering analyses will be defense against liability all the way back to design.

If, in the real world we find system analyses useful, so also will the courts, and they can find them so in negligence, warranty, breach of contracts, evidence.

SESSION I

QUESTIONS AND ANSWERS

DR. CLARK: I am interested in the problem of liability of the vendor from the last speaker. On what basis do you say, at the present time, that this is the situation, when you notice that the percent of defective sales that are going to qualify a builder for settlement, are less than 1%? The National Commission on Product Safety has identified .05% as the typical quality reliability insurance plus settlement costs.

MR. HAYES: I don't think I quite understand your question--or did I just hear the first part of it.

DR. CLARK: Why do you say it is up to the vendor today, that the manufacturer is taking the responsibility for its product?

MR. HAYES: I think you all find that those cases that have resulted in very large settlements and where the cases are completely litigated, (i.e. not settled out of court), that the responsibility in many cases today ends up on the vendor.

DR. CLARK: This is a very small percent of sales! The real responsibility remains on the buyer.

MR. HAYES: All right, I buy that but we are talking about litigated cases. Many airplane cases end up in placing the negligence on the designer of the airplane. This is becoming more and more frequent. It is my point, that adequacy of design is important now in law suits and the courts look at how the manufacturer designed the product to determine whether or not the manufacturer is liable when it is involved in an accident.

DR. CLARK: We were very impressed in the National Commission on Product Safety with what a small percent of the product failures end up in liability suits. Most of these things of course get settled out of court, but it is a very small percent that ends up as the manufacturer's responsibility.

MR. HAYES: Yes, but I think if those products happened to be pressure cookers or other hazardous devices or vehicles that get into the public's hands and create the accidents, I think you will find a larger percentage.

MR. BOLGER: It would be interesting to see how the settlements went too.

QUESTION: Concerning the supervisors reporting on accidents, you seem to indicate that this supervisor knows what the problems are in this management system and you infer a great deal of validity to what this man is saying, how do you know that what he is saying is that valid?

POPE: I don't know that I can take your question and give you the answer that you're looking for. The only thing that the aligned supervisor knows is that things are going wrong. What we've done is, we coded, we have a coding system, and we have given him a number of questions which he can respond to, we literally lead him towards. For example, if he thinks personnel is not giving him a problem or he has a problem, he then has a whole series of things he looks at under personnel and one of them would be staffing. If he has a lifting problem, he can say, well we can go out and train them how to lift, yes, but I should have an extra man there too. He not only puts in that he has a condition of lifting but he also puts in that he has a personnel problem related to staffing. Then, when we go to the computer and ask how many staffing problems we have had in accident situations related to personnel, we then can go back to personnel with a cause and a cost, we go by cost, and say to our personnel function that has something to do with staffing, do you realize that there is a staffing problem generally in this particular area of the organization which is shown by the number of cases that we've got that came out, not necessarily lifting but staffing was the problem in many other instances too. These people are not happy with their staffing situation and it has cost us this amount of money because of it; therefore, you have a responsibility, a concern to solve that particular problem, not me.

QUESTION: I would like to ask Mr. Pinkel about the datafax accessibility. Is it accessible at the present time only to NASA contractors and NASA personnel?

MR. PINKEL: Anyone can request the information he wishes to have. It is available to the community at large, really. No charge is involved.

MR. BOLGER: That is the intent of it isn't it? It is to be used for the nation as a whole, right?

MR. PINKEL: It is for the nation as a whole. Of course, the interest is steered to the aerospace community, but anyone has a right to it.

QUESTION: Would the information be inaccessible to any lawyer to get information for a law suit?

MR. PINKEL: We can't keep a citizen from having access to the bank.

MR. BOLGER: That poses the problem of who is going to put information in it, Right?

MR. LEDERER: Then he can be sure of his facts before he distorts them.

MR. PINKEL: We'll distort them a little first, Jerry.

SESSION II
SYSTEM SAFETY IN AVIATION

Session Chairman - Mr. H. Kurt Strass

"Why System Safety Programs Can Fail"	Mr. Willie Hammer
"The Practical Application of Mishap Data in Army Aircraft System Safety Programs"	Lt. Colonel James T. Darrah, Jr.
"Some Thoughts about Systems Safety Assessment and Its Current Application in Aerospace"	Mr. Peter R. Allison
"Pilot Safety for the X-24A Lifting Body Vehicle"	Mr. John Cochrane

N72-25960

PRECEDING PAGE BLANK NOT FILMED

WHY SYSTEM SAFETY PROGRAMS CAN FAIL

Mr. Willie Hammer

Member

Senior Technical Staff
Hughes Aircraft Company

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

As a participant of the first Air Force-Industry Conference on System Safety in 1963, I remember the aims and claims of the proponents of this new concept; the presentations on why System Safety programs were necessary; and other (hopeful) assurances that System Safety programs would minimize the number of accidents involving new systems. After eight years, I believe we have neither achieved the aims nor fulfilled the claims. This paper will try to indicate why not, and why they can continue to fail. My experience has been with DOD activities, procedures, specifications and standards, and my comments are predicated on that experience. NASA personnel will probably be able to correlate those comments related to DOD with their own practices and problems.

Let's start at the beginning, with the initial requirement for a System Safety program in a Statement of Work.

The item which can contribute most to failure of a System Safety program is ambiguity, lack of clear definition, use of obsolete requirements, and pure typographical errors in a poor Statement of Work.

This leads me to a set of axioms regarding contractors efforts. They apply to contractors for ditch-digging, the aerospace industry, or any other activity. They are not intended to be derogatory; they are merely basic facts of life which everyone should understand.

Axiom #1 - No contractor will accomplish a task unless he is specifically and contractually required to do so.

Axiom #2 - No contractor will include in a proposal for a contract any uncalled for effort which will increase his cost so he might not be awarded the contract.

Axiom #3 - Any requirement which is not clearly stated will be interpreted to the best advantage of the contractor.

Axiom #4 - A contractor will pay more attention to a requirement which stipulates a penalty for noncompliance, than to a requirement for which no penalty is indicated.

When MIL-STD-882 was being coordinated, some engineers argued (and won) that no other specifications or standards should be referenced; they should be included in the Statement of Work. Frequently they are not. Some Statements of Work still refer to specifications and standards which have long been rescinded. Add typographical errors, and the problems grow even more complicated. I have seen AFR 127-100, Responsibilities for the Explosives Accident Prevention Program (which involves relationships between the Air Force and the Armed Services Explosive Safety Board), with which the contractor has no concern, cited when AFM 127-100, Explosives Safety, was meant. Axioms #1 and 3 apply in such cases.

An especially miserable requirement I have seen in a Statement of Work is: "The principles in AFSC DH 1-6 will be observed." What principles? I found one ------- and it was wrong. (In Design Note 4B2: Fuel/Propellant Equipment, it states: "Component design and selection must be based on the fail-safe principle, i.e., failure will cause minimum system degradation." Actually, the fail-safe principle is: first and foremost to prevent injury; secondly to prevent damage; and lastly, to prevent system degradation.)

Next I would like to propound "Hammer's Law": The probability of failure of a System Safety program varies directly as the square of the time from system concept until a firm, clear, funded System Safety requirement is issued in a Statement of Work. If the requirement isn't in early, there may be problems; if it is left until the end of development, don't expect much. It is easier to guide designers into safe practices than it is to change prepared designs.

Another detriment to the success of any System Safety program is the use of "weasel" words in Statements of Work, specifications, standards and other criteria. Safety requirements are indicated and then qualified by a following phrase, such as "as far as practicable" or "if practical". Or a paragraph will state: "Designers should consider the following:" and then list requirements. The designer considers them and then decides he'll stick to Axioms 1 to 4. If the procuring activity believes there is a valid requirement, it should be stated clearly, firmly and without qualification. If the contractor cannot meet the requirement or wants to deviate, he should request approval from the procuring activity.

Unless the safety requirements are stated clearly, and where they are readily apparent as firm requirements, some of them will be overlooked by designers. The Air Force has

placed much of its reliance for this on AFSC DH 1-6, which I believe failed miserably. The best document I have seen to this purpose is the Navy's MIL-S-23069(Wep), Safety Requirements, Minimum, For Air Launched Guided Missiles. It was issued in 1961 and requires updating and other revisions, but even now is very useful.

The next major problem to accomplishment of a good System Safety program is MIL-STD-882 itself. The original System Safety specification, which applied solely to the Air Force, was MIL-S-38130. It was prepared in the Directorate of Aerospace Safety at a time when the Air Force was receiving new missiles and putting them into operational use with little prior warning of their hazards, and with inadequate safeguards. Some of the propellants were considered so toxic, reactive, and explosive that the Air Force hardly wanted information on them revealed to the general public. MIL-S-38130 was therefore prepared to alert Air Force safety people against the next hazards coming down the pike; and secondly, to permit safeguards to be provided during development. The Gross Hazard, and now Preliminary Hazard, analysis was stipulated; primarily for the alerting process, and then to initiate action to provide safeguards. This procedure has generated problems and should be updated.

I have contended for a long time that any system (or product) will have only a limited number of factors which will directly cause injury or damage. I call these "primary" hazards. There are numerous and various contributory factors to each of these, but the primary hazards are limited. This is true whether an aircraft, space station, skateboard, tank, radar or washing machine is being considered.

Figure 1 is a Safety Consideration Tree for a submarine, prepared to illustrate this contention. It is indicative of what can be done. People more knowledgeable of submarines can probably improve it. The block on "Injury" can be expanded in a manner similar to the one on "Damage". The trees are easy to prepare, and should be prepared by the procuring activity for each system for whose development it is responsible. After a few iterations and reiterations, some fine trees will result. Information derived from them can be put to many uses:

a. The various factors which can affect safety and which must be considered in the development of a system or product are readily apparent. There will be no need for a Preliminary Hazard Analysis. The first advantage to this is that it will eliminate a sore point for competing contractors. No contractor likes to point out that hazards exist in his system. A contractor with the better System Safety engineer might be able to point out more hazards, making his design appear more dangerous, than that of a competitor with a less knowledgeable System Safety engineer. With this method, the contractor will not have to make a Preliminary Hazard Analysis. He can get on with his more detailed analyses.

b. MIL-STD-882 now requires a Preliminary Hazard Analysis be prepared for use in the next phase of development. If one wasn't prepared in the previous phase, a problem arises. With the concept I envision, the procuring activity will indicate the problem areas which they have established from the Safety Consideration Trees; the contractor indicates in his proposal how he will handle them; the procuring activity either approves or requests more satisfactory information until it does approve; and things get started immediately, in the current program. This method can be used even in the Concept Phase where the contractors would be required to indicate their provisions for safety for each of the problem areas, in their system specifications. This is the point at which incorporation of safety requirements is needed most. Remember Hammer's Law!

c. When contractors are given the same firm requirements on which to estimate and prepare their System Safety efforts, they will be more comparable. The effort, manpower and cost of each task can be broken down and evaluated more easily. The procuring activity will also find proposals easier to evaluate if they are consistent in substance.

There are other advantages to use of a method such as this:

- *Data files can be established using the same coding as that shown on the trees.
- *The Armed Services can ensure that each factor or problem is covered by a suitable

requirement for safety in a military specification or standard.

*Personnel working on any program can be assigned to those problems which they are most capable of handling.

*It is a logical method of attacking safety problems, instead of waiting until a problem jumps out of the bushes.

MIL-STD-882 creates more problems. The use of the four hazard categories is a case in point. Those categories generate more problems than they are worth. First of all, they require clarification if they are to be used for any purpose. What is meant by "major system damage" or "severe injury"? If the various categories are defined well enough by each procuring activity to indicate clearly what they want them to mean, you will have a Preliminary Hazard Analysis.

The second problem with the four hazard categories is that too much time is spent trying to decide into which category each problem falls; and then to justify the choice. There are other reasons for which the categories should be eliminated (they overlap, detract from the effort of minimizing and controlling hazards, etc.) which will not be discussed here.

MIL-STD-882 applies to System Safety programs; it has no technical safety requirements, such as MIL-STD-454. If the technical requirements are not included in the Statement of Work, or by the contractor himself (watch out for Axiom #2), they will not become criteria to be observed. A solution is to require the System Safety Program Plan to be submitted as part of the contractor's proposal. Even better, this proposal should be submitted as a separate line item.

One more point about MIL-STD-882 and the Plan: AFSC Form 1664 for Contract Data Requirements states that the Appendix to MIL-STD-882 "shall be used" when preparing the Plan. Since the Appendix and the text of the standard do not jibe, it generates problems. Contractors observe the four axioms I have presented; but when a requirement is presented, they are very conscientious about its observance. So when a requirement says "shall" they want it that way, even if we System Safety engineers say that MIL-STD-882 cites it as a sample, and that it is not very good, they still want it that way because the 1164 says "shall."

I don't have many gripes about managers, especially when I realize they are acting within the four axioms I pointed out. Other than that I can only say that contractor (and maybe procuring activity managers too) have a hard time understanding that System Safety engineering extends beyond the safety considerations of design, reliability, maintainability, and human factors engineers. And very frequently it requires a redirection of their thinking when we indicate that System Safety includes minimizing damage of hardware, which was formerly a responsibility of reliability.

Often, this results in a failure to support the System Safety program properly. Another management solution is to appoint one or two men as a System Safety organization, and to direct that representatives in various design groups, systems engineering, test, reliability, maintainability, and other functional areas will perform the necessary System Safety tasks for their organizations. From what I have seen, it doesn't work. Everyone may be very conscientious about it, but such an arrangement does not work.

The last problem I have encountered with managers is that many believe that any requirement involving probabilities, such as a quantitative safety analysis to determine whether a specified level is being met, should be handled by the reliability engineers. Perhaps they believe System Safety is an extension of the hard hat-hard shoe school of safety and that System Safety engineers know nothing about the more theoretical aspects of engineering.

Some of these problems with management may actually be due to the System Safety engineer:

a. Many have not gotten beyond the 1963 stage when talks were common on "Why System Safety Is Needed." (If there is no System Safety requirement in the Statement of Work for a contract, there is no point in bringing up "Why System Safety Is Needed." Begin looking for work elsewhere.) System Safety engineers have done little to advance this discipline to a point where it can be recognized as something different from reliability and human factors. (Perhaps like Moses in the desert after the Exodus from Egypt, we need a new more energetic generation to take over, to forget the past, and accomplish new things.)

b. Many System Safety engineers don't know where to start a program or analysis. They then do either of two things: wait for something to rise up out of the bushes with which they can struggle; or they get onto the paperwork and meeting treadmill. They attend meetings and then write memoranda on the safety aspects. In between, they review the masses of papers which deluge them if they on the paper route. To these people, the approach I have indicated may be helpful in trying to figure out which way to go.

c. Some System Safety engineers are ardent proponents of checklists (I used to be one). Actually, checklists are ineffective for many reasons. Generally they are too late: the design has been agreed upon and frequently accomplished; often they are too general (DH 1 - 6 is in this category); and lastly, if they are not based on firm requirements (Axiom #1), it is generally difficult to have the designs changed.

This paper has gotten rather long. In summation, I will say that if there is one thing which can make a System Safety program fail, it is lack of clarity:

*Lack of clear requirements by the procuring activity.

*Lack of clear understanding of System Safety by other managers.

*Lack of a clear methodology to be employed by System Safety engineers.

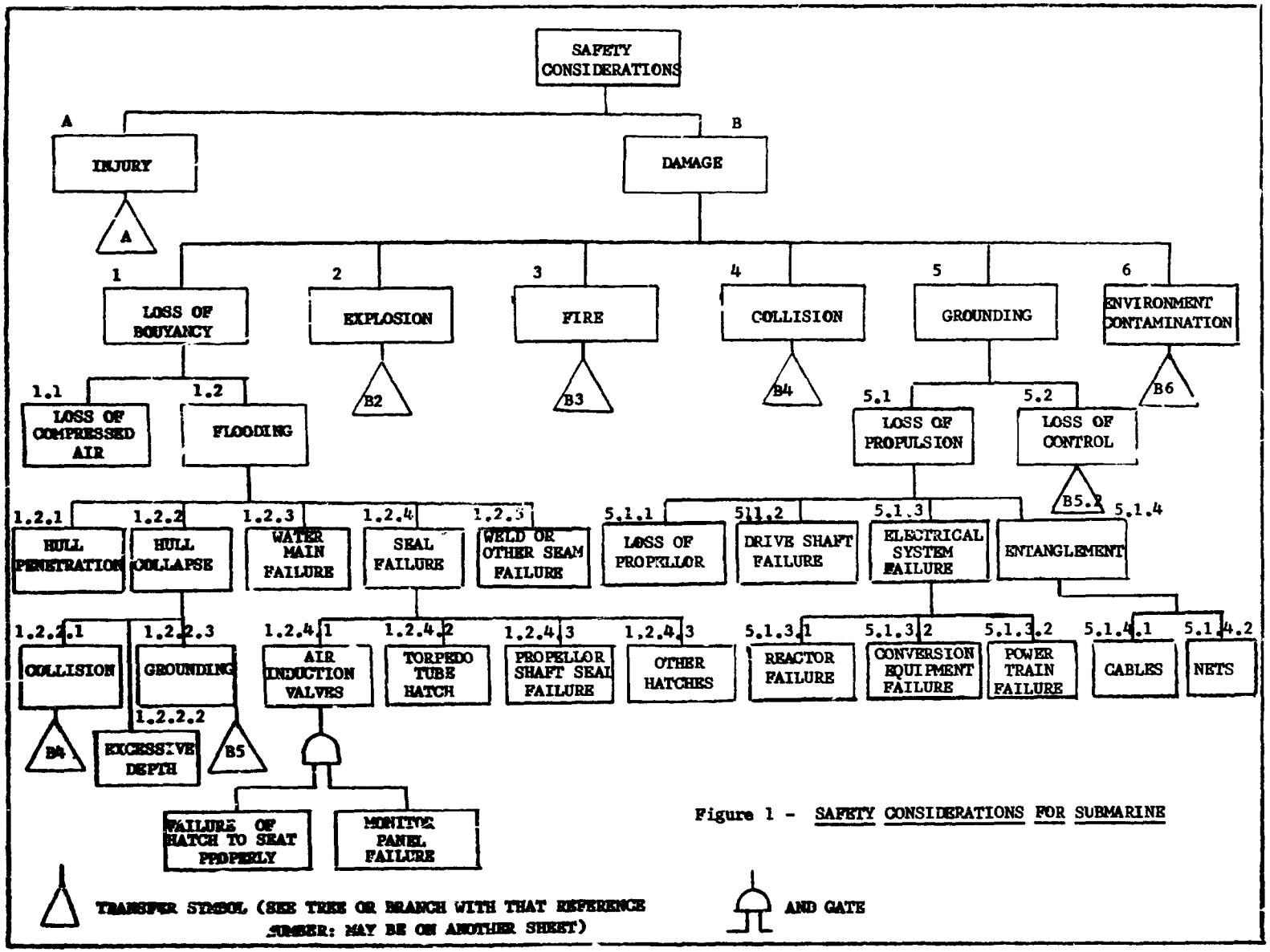


Figure 1 - SAFETY CONSIDERATIONS FOR SUBMARINE

FIGURE 1

N72-25967

THE PRACTICAL APPLICATION OF MISHAP DATA IN ARMY AIRCRAFT SYSTEM SAFETY PROGRAMS

Lt. Colonel James T. Darrah, Jr.
U.S. Army Board of Aviation
Accident Research

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

The system safety discipline has existed for several years now as a rather well defined concept. There has been very little argument as to the desirability of the system safety objectives. In fact, among many of those who know what these objectives are, there even has been generated a fair amount of what can only be described as "religious fervor" at the prospect of achieving the goals of system safety. But, with its well-organized, logical and comprehensive approach to accident prevention, the application of the system safety concept in practice has not been as rapid and effective as its attributes would warrant.

The United States Army Board for Aviation Accident Research (USABAAR) is vitally concerned with the application of system safety, particularly with respect to new developmental Army aircraft programs. USABAAR serves as the central agency for the Army Aviation Accident Prevention Program which includes the receipt, processing and analysis of all data and information related to Army aircraft accident experience. This paper discusses the means by which USABAAR now utilizes this vast store of historical accident data in the application of the system safety concept for developmental aircraft. While the methods described here admittedly fall short of realizing the full potential benefits of using our past accident experience, we feel that significant steps have been made in that direction. As more experience is gained in the application of these methods, certainly many refinements and improvements will follow.

The history of an accident can be generalized and simplified as shown in Figure 1. This depiction will be used throughout the remainder of the paper as methods are discussed which pertain to each segment of the diagram.

REQUISITE CLIMATE

Requisite climate, or "hazardous conditions" as it might be called, indicates that the stage for an accident must be properly set. If the proper conditions are not present, no accident will occur. These conditions involve the familiar triad of accident factors: man, machine and environment; plus the overall factors of command, management and supervision.

The command or management influence existing in an operation may play a significant role. Some casual remark by the commander at a morning briefing may quite innocently start a chain of events leading to catastrophe. Such influence most likely will concern the urgency of the mission to be performed, the quality of results desired or the belittling of problems, obstacles and risks. The result may be that the impression of "accomplish the mission whatever the cost" is conveyed which is tantamount to indorsing recklessness.

The condition of the people involved is perhaps the most complex factor present. The physical condition, state of mind, morale, proficiency and a wide variety of physiological and psychological factors all interrelate in a complex way to affect the potential human involvement in an accident. Change one small item and an accident could be averted.

The condition of the machine also involves a highly complex functional relationship of hardware which must exist in just the right way before an accident can occur. This relationship includes maintenance practices, worn pieces/parts, age of the equipment, design deficiencies, operating limitations and others, the complexity with newer sophisticated aircraft.

Environmental conditions cover an extremely broad range of phenomena including weather, terrain, operational situation, air traffic control airfield facilities and many more. The true influence these conditions on accidents is most often either not known or ignored.

MANIFESTATION OF HAZARDS

The worst possible combination of all the conditions listed above could conceivably exist and no accident would result unless some hazard manifested itself. Given the requisite climate the manifestation of the proper hazard initiates the accident sequence. This sequence can usually be divided into two or more main occurrences, precipitating and sustaining events.

The sequence will start with some trigger event which can be produced by a staggering variety of causes; again involving man, machine, environment and management or any combination of the four. Until this time, the

factors present in the requisite climate have played a passive role in the accident where the cause-effect relationship is usually not very precise. With the occurrence of the trigger event, however, the sequence of events which follow is usually quite predictable. What was a potentially hazardous condition before will now manifest itself through some event which, in itself, may never be considered hazardous. For example, shutting down one engine in a twin engine aircraft at altitude may present no hazard whatsoever. Shutting down that same engine while on short final approach during an emergency landing because the other one failed earlier could - - - and did - - - have catastrophic consequences.

Rarely does an accident occur as a result of one single event. There is usually a series of several events which follow the trigger event in sequence up to the accident itself. These can be called "sustaining events". If they do not occur, the accident sequence is broken.

Thus, given a requisite climate or potentially hazardous conditions, the accident sequence begins with a trigger event, is carried forward through sustaining events and an accident occurs.

UNDESIRABLE EFFECTS

If all this just described did not produce consequences which we wish to avoid, there would be no safety effort at all. It is really the undesirable effects of accidents themselves which justify our attempts at accident prevention. If this statement seems a trifle too basic and should have gone without saying, consider the possibility that we as safety specialists may have tended to lose sight of these undesirable effects of accidents as our basic motive force. Perhaps we have not concentrated sufficient attention on all the adverse consequences we are trying to preclude. We allow ourselves to become completely absorbed and obsessed with safety techniques, methodology and philosophy for their own sakes without maintaining a clear view of our ultimate objective - minimizing these efforts.

The effects of accidents can be grouped into two general areas with the respect to time. First, the abrupt damage and destruction to materiel plus injury and death to personnel are the immediate consequences of an accident. Accidents are classified as to the degree of severity of these immediately observable effects. MIL-STD-882, the system safety standard, categorizes hazards in terms of their potential effects on materiel and personnel should an accident result from the hazard. But such categorization is not the end event; in a sense, it should be only the beginning of the analytical process to determine effects of accidents.

The second grouping of consequences from accidents includes the long range effects, those perhaps not immediately observable and which have an impact far beyond the time and geographical location of the accident itself. To the Army, these effects add up to a total cost in terms of lost or degraded mission effectiveness or capability. It is not at all farfetched to say that <u>each</u> aircraft accident, no matter how insignificant in terms of immediate consequences, has some adverse effect on the capability of the Army to accomplish its mission. It logically follows, then, that if the total number of aircraft accidents is substantial, then the impact on mission effectiveness also will be substantial.

At any given point in time the accomplishment of the Army mission requires that certain aviation resources, people and materiel, be available. The degree of non-availability of these resources logically has a direct bearing on the ability to accomplish the mission . . . . mission effectiveness. Since we obviously cannot acquire these resources instantaneously, we must not only project what our missions will be in the future, but also estimate what total aviation resources will be required in light of that future mission. Such estimates and projections are made for as far into the future as practicable and are then refined as time goes on. It is an extremely complex process, not the least part of which involves projecting the status of the current aircraft inventory, aviation personnel and facilities situation. Any shortfall of quantity, quality or capability in our projected inventory, personnel or facilities compared with our estimated requirements gives the basis for planning to acquire these resources. If we err, and underestimate our losses in aircraft and personnel, for instance, or do not adequately provide for quality in new aircraft,

an adverse impact on mission effectiveness is the result.

The main thrust of USABAAR's use of accident data for future aircraft programs is to estimate the long range impact on mission effectiveness through the proper analysis of this data. Unless we fully consider the far-reaching effects of accidents on people and materiel, we are not fulfilling the objectives of the system safety discipline.

ACCIDENT DATA

Accident prevention programs have traditionally operated on the basic premise that if the causes of accidents could be determined, preventive measures could then be developed to eliminate the causes. Following this premise, the primary task has been the acquisition of data and information through an accident investigation and reporting system. This task is performed exceptionally well today. Several years of diligent sleuthing, exhaustive interviewing of witnesses, and even precise laboratory analysis by both highly skilled and amateur investigators have produced an immense store of data and information on the causes of aircraft accidents. A significant portion of the safety effort of all military services, the Federal Aviation Agency, the National Transportation Safety Board and civilian aircraft manufacturers and operators is devoted to merely processing this wealth of data and information.

The results of accident investigations have usually been recorded in the form of a description of the accident sequence of events: the confirmed or suspected cause factors; recommendations to prevent recurrence and general factual data such as date, time, place, type aircraft, crews members, injuries, fatalities, etc. In general, the immediate consequences of the accident are recorded along with the events which led up to the accident. Quite often, but not always, it is possible for a thorough investigator to delve far enough into the past to well define the hazardous conditions which existed some time prior to the accident thereby enabling the accident to occur.

Until fairly recently, the primary use of all this data was to provide a source for various totals and rates reflecting only the most general accident information. The key parameter for safety has been the periodic accident rate, the number of accidents divided by the number of hours flown. Accident "costs" have been reported by totalling acquisition "book value" for destroyed aircraft and repair costs for damaged machines. Fatalities have been totalled as have injuries, but with various criteria being used to describe severity of injuries. Cause factors have been lumped into a very few categories which then have been totalled. Among the most usually cited factors are crew error, materiel failure or malfunction, weather and maintenance error. Degrees of severity of accidents have been classified from "total loss" to "incident" depending on the extent of damage and injury.

Certainly, this most general treatment of accident data had a significant impact several years ago when compared with the even earlier situation when nobody even knew how many accidents they had been having. Initially, the concentration of attention on safety supported by only the most superficial analysis of accident data produced dramatic improvements. The magic "accident rate" began to drop rapidly as if to prove conclusively that such measurement of the problem was all that was necessary to solve it.

IMPROVED DATA SYSTEM

These methods which served the cause of accident prevention so well in the past are no longer adequate. There are widespread efforts underway for the development of more sophisticated data systems for safety. These efforts show that traditional parameters used to measure mishap experience cannot be used directly to solve many accident prevention problems today. Only a few deficiencies which have caused accidents in existing aircraft can be pinpointed sufficiently to correct the problem. For the rest of the problems in existing aircraft and for all of the potential hazards in a developmental aircraft, the identification of these old, generalized parameters does little but indicate a broad area of interest in which detailed analysis and specific evaluation is required. The detailed effects on mission capability must be identified to justify corrective action and the cost of such action.

2.-5

To enable USABAAR to respond in this manner, completely revised accident reporting forms have been developed and put into use recently which greatly expand the scope and detail of information provided as a result of investigation of the accident are recorded along with the events which led up to the accident. Quite often, but not always, it is possible for a thorough investigator to delve far enough into the past to well define the hazardous conditions which existed some time prior to the accident thereby enabling the accident to occur.

Until fairly recently, the primary use of all this data was to provide a source for various totals and rates reflecting only the most general accident information. The key parameter for safety has been the periodic accident rate, the number of accidents divided by the number of hours flown. Accident "costs" have been reported by totalling acquisition "book value" for destroyed aircraft and repair costs for damaged machines. Fatalities have been totalled as have injuries, but with various criteria being used to describe severity of injuries. Cause factors have been lumped into a very few categories which then have been totalled. Among the most usually cited factors are crew error, materiel failure or malfunction, weather and maintenance error. Degrees of severity of accidents have been classified from "total loss" to "incident" depending on the extent of damage and injury.

Certainly, this most general treatment of accident data had a significant impact several years ago when compared with the even earlier situation when nobody even knew how many accidents they had been having. Initially, the concentration of attention on safety supported by only the most superficial analysis of accident data produced dramatic improvements. The magic "accident rate" began to drop rapidly as if to prove conclusively that such measurement of the problem was all that was necessary to solve it.

IMPROVED DATA SYSTEM

These methods which served the cause of accident prevention so well in the past are no longer adequate as evidenced by the comparatively recent development of more sophisticated data systems for safety. The traditional parameters used to measure mishap experience cannot be used directly to solve many accident prevention problems. Only a few deficiencies which have caused accidents may be able to be pinpointed sufficiently to correct the problem. For the rest of the problems in existing aircraft and for all of the potential hazards in a developmental aircraft, the identification of these old, generalized parameters does little but indicate a broad area of interest in which detailed analysis and specific evaluation is required. The detailed effects on mission capability much be identified to justify coorective action and cost of such action.

To enable USABAAR to respond in this manner, completely revised accident reporting forms have been developed and put into use recently which greatly expand the scope and detail of information provided as a result of investigation. The new forms were designed to take maximum advantage of a vastly improved data processing capability at USABAAR using a large digital computer. A completely new management information system has been constructed around this computer and is now in use.

It was realized early in the planning stages of the new USABAAR data system that it would not be good enough if all the computer could eventually do was produce the same sort of totals and rates produced previously. One skeptic, early in this planning stage remarked, "We're going to be able to arrive at the same, old general conclusions . . . only faster!" It has not worked out that way for one basic reason. The speed of the computer has enabled the efficient processing of timely data in far greater detail than ever before. This is the key to the success of a modern accident data system.

The production of this much more definitive data already has significantly improved our capability to do the following:

a. Conduct in-depth studies and analyses to determine the long-range effects of accidents.

b. Clearly define the sequence of events and the mechanism by which hazards manifest themselves.

c. Comprehensively define the hazardous conditions which must exist prior to initiation of an accident sequence.

d. Pinpoint areas for specific corrective action, specify the action required and establish priorities for action.

e. Forecast measures to limit the requisite climate and inhibit hazard manifestation while at the same time placing such actions in context with their influence on the long-range undesirable effects of accidents.

DEVELOPMENTAL AIRCRAFT

We have recently developed methods by which this expanded capability can be applied "before-the-fact" to developmental aircraft systems. It is here that the most fertile application of our management information system is to be realized. These methods have shown that the gap can be successfully bridged between historical accident data on a fleet of existing aircraft in various stages of obsolescence and potential hazards in future aircraft which now exist perhaps in concept only.

The system safety discipline furnishes us with the overall management tool by which we can optimize the conservation of resources through the prevention of accidents before they happen, that is, to design safety into our aircraft systems. The heart of this process is hazard analysis in which the system is examined in a methodical, comprehensive way at each stage in its development to isolate hazards present. At some point in time, however, the moment of truth arrives when decisions have to be made as to what to do about hazards identified through analysis. Sometimes there is no penalty to correct or eliminate a hazard. Sometimes the hazard is so great that its elimination is mandatory regardless of the penalty. But the vast majority of hazards which are identified through system safety analysis fall somewhere in between. The question then becomes, "How bad do we want to eliminate these hazards?" Heretofore, the system safety engineer could only fall back on the MIL STD 882 category he has assigned the hazard. He has not been able to relate this hazard to future adverse long range consequences. His categorization has only addressed the immediate effects.

History has shown that new operational aircraft systems rarely incorporate a very large number of advanced technological features. Rather, new aircraft represent rational growth versions of previous aircraft with improvements being made where practical and high technical risk features being held to a minimum consistent with performance requirements. The point is, in dealing with new systems, there is usually not that much really "new" about them. Those features of a developmental aircraft which are not new provide the place where accident data on previous systems is most directly applicable.

It is logical to expect that previous accident experience will be used in the design and operation of new aircraft so that cause factors noted in the past will not recur. To a disturbing degree, this has not been the case. There are several instances of the same feature which caused accidents in earlier aircraft being duplicated in newer models. One good example is the use of "redundant" systems in critical areas. Acknowledging that loss of hydraulics for flight controls would be catastrophic, one fairly recent design provided for two hydraulic systems, including two pumps - both driven by a single shaft of inadequate strength. Another design approached the same problem by also providing two hydraulic systems, but with all the hardware and plumbing co-located greatly increasing the chance of double failure from one event.

Such deficiencies as these were not negligently designed into the new system. Perhaps such designs were the result of ignorance - designers just didn't know we had supposedly already learned that lesson. More likely, however, it was probably felt that previous accident experience of one type of aircraft just did not apply to the "new" aircraft on the drawing boards.

This applicability of accident data is a real problem when trying to justify certain safety features in a yet unborn aircraft. USABAAR came face to face with this problem a few years ago when we attempted to prove, through accident statistics, that the Utility Tactical Transport Aircraft System (UTTAS) should have two engines. Since we had no twin engine utility helicopters in the inventory, we used accident data from the CH-47 Chinook, a twin engine light cargo helicopter and compared that data with the single engine UH-1 Iroquois data. As it turned out, one model of the UH-1 actually had a better accident rate than the CH-47. Obviously, this did our argument no

good. Other comparisons, using available accident data, showed some advantage for two engines, but not in the clear cut manner we thought it should. When the case was presented for decision, our arguments were unconvincing. We were told our reasoning was essentially faulty since a CH-47 differs so greatly from a UH-1 that they just could not be directly compared. They are of different size, have different missions, and do not even appear in the inventory in comparable quantities. In short, we had attempted to compare "appies and oranges to justify peaches."

This setback caused us to seriously ponder the factors which would make a difference in decisions such as for the twin-engine UTTAS. Our conclusion was that accident statistics just do not speak for themselves. The development of improved analytical techniques for processing accident data could not stop short of assessing the long range impact of accidental losses. Whereas, for the UTTAS question, we had compared single vs. twin engine accident rates, materiel failures, injuries, and deaths, degrees of damage and costs; we could not estimate, for example, the number of single engine UTTAS aircraft that would be lost due to engine failure and how those losses would affect the number we had to procure initially. This kind of estimate would have had a direct bearing on the decisions being made.

Today, USABAAR is carrying its analytical work several steps farther than before and doing it in much greater detail. While there is much work yet to do, progress has been made in several significant areas.

One area much in need of improvement is the design of future aircraft systems for the specific environment in which they are intended to operate. This consideration is not new, in itself, but the detail to which the operating environment must be specified is new. A major effort is now underway to clearly define the environment in which Army aircraft are expected to operate in the future. Given this definition, USABAAR is now in a better position to identify the specific environmental conditions which favor accidents and to specify detailed design criteria to counter these conditions.

Besides the greater detail now reported from accident investigation, there is another significant improvement which has been made in our data system. A uniform method has been developed to translate the complex details of each mishap into data which can be stored and retrieved by the computer without losing the essential ability to differentiate between the details of each accident. Called "ABACUS", which stands for Aircraft Basic Accident Causes, U.S. Army, this method prescribes a vocabulary and syntax for encoding cause factors of aircraft accidents using a key word concept. Coding of accident information used to be a matter of fitting each set of circumstances to one of a limited number of rigid preconceived statements which seemed to best describe the event. Obviously, this procedure did not allow for distinction between similar situations where the differences were highly significant when it came to specifying corrective action. ABACUS, on the other hand, allows for nearly complete freedom to record the specific circumstances surrounding each individual mishap.

Statements concerning accidents are constructed using approximately 650 key words and phrases. They are combined in a prescribed sequence to describe phase of operation, subject, action verb, subject manner, subject position and/or condition, main object, object qualifier and reason. In addition, to these key words and phrases, aircraft nomenclature is also included using an abbreviated version of the aircraft parts catalog system. While the number of data elements available for use is still somewhat limited, the system allows for an extremely large number of possible combinations.

Probably most important is the fact that retrieval of data in a usable form is greatly facilitated through the use of ABACUS. Depending on the purpose of the analysis to be performed, any combination of ABACUS words, phrases or aircraft descriptors can be used as an argument with which to query the data bank. This exceptional flexibility in output means that the entire data base can be focused rapidly on virtually any conceivable accident prevention problem. We are no longer limited by inadequate or unusual data but only by our imagination in how to use the available data.

Using the matrix generating capability of the computer, we have greatly expanded our ability to compare the more detailed elements of information now acquired through accident

investigation. From the large number of possible combinations, relationship, between the most significant data elements have been established as indexes for various areas of interest.

One such area is fire in aircraft. A "Fireworthiness Index" has been developed which measures all detailed factors relating to the incidence of aircraft fires and the immediate and long range effects. This index is established for each type, model and series aircraft in the inventory so that rankings between aircraft can be obtained. All the known elements in Fig. 1 are included. Given the detailed insight into past fire experience specific operations and aircraft configurations are then evaluated to determine those conditions which affect the index. The specification of fireworthiness criteria for future aircraft, then, follows this evaluation directly. Furthermore, a relative priority can be attached to these criteria based on the fireworthiness index. For design criteria, the "index" approach is being used to make recommendations in terms of alternatives expressed as functions of the long term impact on mission effectiveness. At present, these recommendations are mostly general in nature, but as our analytical studies are completed, more specific criteria will be developed. For developmental specifications, in addition to the estimate of long range impact, we will make recommendations in terms of alternatives expressed as functions of program costs, schedule and system performance. Such estimates will be of maximum benefit to the project manager and as such, maximize the effectiveness of system safety efforts in a program.

This has been a very general discussion of how USABAAR has begun to solve the difficult problem of using historical accident data in new developmental aircraft programs. By this discussion we do not wish to minimize the importance of continuing to develop improved analytical methodologies. More sophisticated techniques employing better predictive and quantitative procedures are sure to find widespread use in the future. We feel that the surface has only been scratched and that we have embarked on a course that will lead us eventually to the most effective attainment of the system safety objectives.

REFERENCE

Spezia, Emil, "ABACUS", U.S. Army Aviation Digest, October 1970, p. 50.

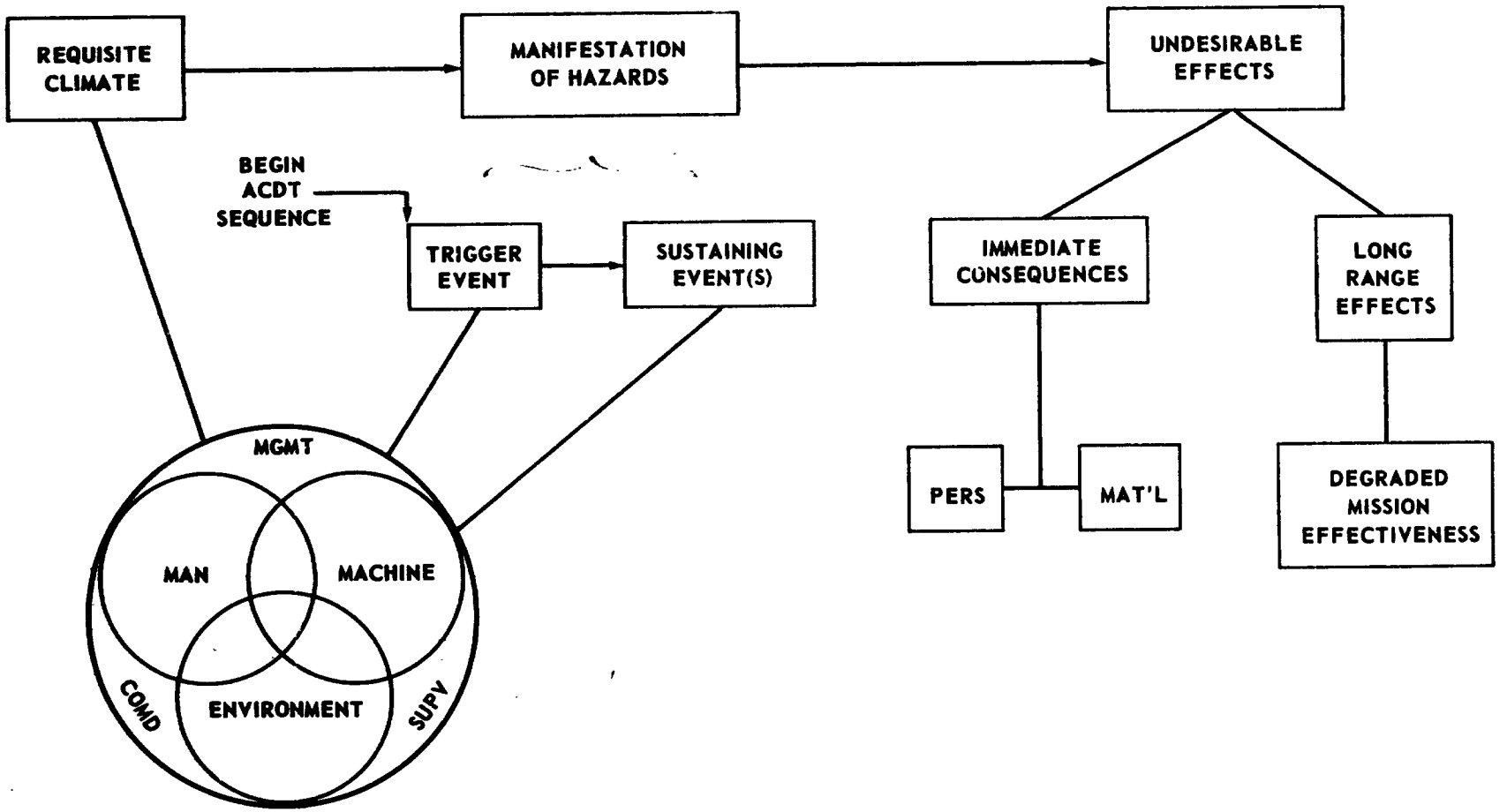

REQUISITE CLIMATE
MANIFESTATION OF HAZARDS
UNDESIRABLE EFFECTS
BEGIN ACDT SEQUENCE
TRIGGER EVENT
SUSTAINING EVENT(S)
IMMEDIATE CONSEQUENCES
LONG RANGE EFFECTS
PERS
MAT'L
DEGRADED MISSION EFFECTIVENESS
MGMT
MAN
MACHINE
ENVIRONMENT
COMD
SUPV

FIGURE 1

N72-25968

SOME THOUGHTS ABOUT SYSTEM SAFETY ASSESSMENT AND ITS CURRENT APPLICATION IN AEROSPACE

Mr. Peter R. Allison
Design Surveyor, Responsible
for
Systems Coordination
British Air Registration Board

Presented at the

NASA Government-Industrt
System Safety Conference

May 26-28, 1971

PRECEDING PAGE BLANK NOT FILMED

SUMMARY

As the title implies this is a discussion of various issues and requirements which must be considered during the actual work of Safety Assessment, and does not deal with all the aspects of a complete programme.

The task and its objectives are considered and the importance of presentation is stressed, so that problems and their solution are displayed adequately to the many disciplines involved. The definition of areas of influence to which the requirements can be applied and for which safety objectives can be derived, is discussed. The use of rational requirements is considered in this context, as is the use of numerical methods in the exercise of judgement.

It is also emphasized in the course of this paper that the assessment is a discipline which directs the appropriate skills at the problems as required, and must never be interpreted as a means of replacing these skills.

CONTENTS

1 INTRODUCTION

Much has been said on both sides of the Atlantic on the subject of Safety Assessment, and, in fact, it is probably right to say that it has all been said. There is for example, a lot of information published by various Government Agencies, which has been written as part of their procurement activities, and this has been of immense importance with its emphasis on the orderly application of safety analysis. However, it is thought to be generally true that although all the material is there in advisory form, its application is subject to much freedom of interpretation, and assessments have been made within these frameworks at many different levels, and perhaps with varying objectives. It seems opportune, therefore, to take another look at the complex path through the safety assessment process, as simply as possible, with the object of highlighting the principles involved.

Discussion can range from the administrative structure necessary in the manufacturing company down to the specific statistical techniques required to deal with the validity of a test programme; from the type of personnel required in a safety organisation and the methods employed to make the biggest impact, or, perhaps, the influence of the computer on the safety programme. Problems of documentation and format are by no means unimportant in this subject and have been discussed in depth. Many other aspects merit separate consideration and all can have a major influence on the approach to safety. This rather daunting appreciation of the field emanates from my work in the European aircraft industry and from a recent opportunity to look at safety assessment in a variety of American Aerospace organisations and is given to emphasise the fact that the subject matter of this paper is strictly in line with its title. Consequently, I propose to touch upon various issues and requirements which must be considered during the actual work of Safety Assessment, with the intention of stimulating discussion of the basic approach which should be made.

2 SAFETY ASSESSMENT TASK

The Safety Assessment task is to ensure that the design, construction, and operation of the device being investigated is sufficiently safe for its projected use. This requires the assurance that all foreseeable faults and critical situations have been adequately taken into account. Critical situations will include any such conditions which may arise when systems are working in the fault free mode and must take account of external events.

The demands of a statement such as this are immense and, apart from the application of the engineering and other skills involved, have given rise to the creation of many procedures involving different logic and documentation in order to assist in its satisfaction.

If we endeavour to state with more precision the process necessary to carry out the task the following requirements arise:-

(a) To define the safety objectives.
(b) To display the design, construction, and operation of the vehicle in such a manner that its potential weaknesses are clearly revealed.
(c) To ensure that the best judgement in the skills relevant to the problem and its interfaces has been brought to bear.
(d) To show to the satisfaction of all concerned that the safety objectives for the complete vehicle and its operation have been met.

If the Safety Assessment satisfies these requirements the detailed procedure is not important and depending upon the technology involved, and the possible hazards, many perfectly adequate methods are available. However, because of the contributions of different technologies to aerospace vehicles, some standardization on a given project is obviously desirable. In particular a standardised approach to safety assessment should facilitate the feed back of operating and servicing data, as experience accumulates, so that the aspects can be readily up-dated.

3 DEFINITION OF SAFETY OBJECTIVES

3.1 Background

Where the overall engineering of aircraft components and systems is concerned, safety objectives have been defined in terms of good engineering practice, and this has been implemented by ensuring compliance with arbitrary design rules developed in each succeeding generation of aircraft on which experience has been obtained. Where successive designs have produced relatively small increases in weight and speed it has not been too difficult to continue safety assessment processes which require establishing that good engineering practice is being followed, and the satisfaction of certain arbitrary rules stated in the airworthiness requirements. However, when the designer is asked to produce spectacular increases in speed, weight or airfield performance, an entirely new dependence on particular systems may arise which may have considerable complexity and require a more detailed understanding of the interfaces for safety reasons. In these cases, it becomes progressively more difficult to carry out safety assessments on a subjective basis, related to arbitrary design rules. The fundamental assumptions which have been made in most approaches during the last decade are:-

(a) System engineering can be adequately assessed against the testing and experience gained with previous systems.

(b) Adequate safety criteria can be given in terms of formalised experience and arbitrary statements of good engineering practice.

(c) By complying with these criteria, and using the developing skills of the assessor the aircraft can be made to demonstrate in service a safety record expressed on a basis of fatal accidents per flight or per hour etc. which will be an improvement on previous experience.

It seems necessary to emphasise these points to demonstrate that safety has always depended upon the extrapolation of experience and the use of the designers' skills. The aim should be to provide the best framework of objectives, and techniques of assessment, so that this approach can be continued into areas where additional system dependence, interaction problems, etc., are making the task more difficult.

3.2 Rational Requirements and Major Objectives

We can now say that to give more precision to the statement of objectives and the classification of hazards we will specify a rational system of requirements which we will use in the more advanced applications, and which can be related statistically to the level of airworthiness required when the aircraft enters service.

For example we can consider the airworthiness standard TSS 1-1 which is applicable to Concorde.

The object of this sort of requirement is to erect a framework which allows a more explicit statement of the objectives, hazards and their probabilities than has been usual hitherto. This is not to say that adequate assessments have not been performed, but it is being suggested that it is advantageous to indicate more clearly than in some past assessments why the decisions affecting Safety have been taken.

An important aspect of this, to which reference has already been made, is that service experience can be more readily referred back to the basic design assessment particularly where redundancy has permitted low MTBF.

Very considerable care has been taken with the requirement to allow the various frequency levels to be defined where necessary by analogy or in broad terms, but a numerical scale of probabilities is unavoidable, at least, by implication. Some people have difficulty in accepting this numerical concept, and

I shall return to this subject later when the exercise of judgement is discussed.

4 THE ORGANISATION OF THE ASSESSMENT

4.1 General Approach

The design, construction, and operation of the vehicle should be displayed in such a manner that its potential weaknesses are clearly revealed and it is suggested that this should be dealt with in the following manner:-

(a) Consider the Significant Airworthiness Functions which are required of the complex of systems which together make up the aircraft.

(b) Designate the system boundaries which allow the best logical separation of these functions.

(c) Designate the Zones, or physical boundaries, in which systems, parts of systems, and components are installed.

NOTE: The terms 'Significant Airworthiness Function' and 'Zones' will be discussed in more detail later.

(d) Carry out a system analysis for each of these arbitrarily generated groups by piece part count, for example, or any other desirable approach, in order to validate the significant airworthiness functions.

(e) Ensure that the interfaces are adequately taken into account. This includes interfaces between System, between System and the Zones in which they are contained, aircrew and system interfaces, etc.

As stated earlier, the Certification Authorities must assist this process of logical partition for analytical reasons, by stating requirements which take account of system dependency in a rational manner without unduly restricting the design. In addition, it is necessary because of the great background of experience to retain many features of the existing requirements of BCAR and FAR where their application is practicable for the specific type under consideration. So the aircraft is subdivided into manageable parts on the basis of the significant airworthiness functions, and the zones or compartments in which systems, parts of systems and equipment are installed.

There is of course, a considerable iteration and feedback in this part of the work since many factors are involved. Significant airworthiness functions will be influenced by the impact of the airworthiness requirements on the required operational characteristics. Zones may be determined not only by the structure arrangement but also by disposition of the systems and equipment, and the hazards arising from malfunction and interaction. These aspects will be further discussed. In real cases some compromise with factors outside Safety aspects may be necessary, involving, for example, the extent of subcontract work and particular responsibilities when the project is being carried out by more than one major contractor. It may well be that ability to define and deal with the interface problems may be a powerful factor in the determination of the sub-divisions of systems and zones.

For example, if one considered a supersonic aircraft having variable intake geometry it would be difficult to disassociate the behaviour of the intake, engine and perhaps its variable exhaust nozzles. It is clearly desirable to perform safety assessment on a unit which includes each of these parts and to ensure that this is carried out by an integrated propulsion unit team.

4.2 Discussion of the Significant Airworthiness Function

In the context of this primary activity, the Significant Airworthiness Function has considerable significance when the Safety Assessment is being organised. It is important to recognise that there are many functions which do not have airworthiness significance. These could have powerful commercial implication in the way of effects on

despatch capability, achievement of desired flight profile, maintenance costs, etc., and these functions will also be submitted to exhaustive system investigation which must be separate from the analysis required for Safety reasons. For example if a feature of the aircraft to be investigated is a droop nose necessary to provide the vision required for operation in various flight phases, we could consider two of its possible functions. In one case, the system could fail in a mode which prevented the nose being raised to the supersonic position. The result might be to prohibit flight in the supersonic mode and airworthiness would only be affected by any contribution which might result from a diversion.

A significant function would be the requirement for lowering the nose during the approach, and failure to achieve this would result in an increased load on the pilot and therefore represent an airworthiness hazard. Consequently, the system ability to perform this task is included in the safety assessment and its integrity matched to the importance of this hazard (however in passing there is also an absolute requirement in the case of Concorde that it should be capable of being landed safely after malfunction of the droop nose).

This discussion emphasises the need in all safety assessment work for precision in the identification of the functions which are associated with safety. It has already been said that safety assessment should provided the best display of the weaknesses of a project and this requirement will not be satisfied by an approach which endeavours to take account of every failure when many of these do not affect safety.

4.3 Integration of the Safety Assessment

At this point we have discussed the requirements and defined the systems and zones necessary for their logical application. The systems will then be analysed on the basis of single failures and the zones on the basis of detailed checks against installation rules.

These analyses are now developed through the following stages, which are probably sufficiently self explanatory in the context of this paper:-

(a) The system single failure analysis.
(b) The system safety assessment.
(c) The aircraft safety assessment.

These stages facilitate the grouping of piece part failures, the combination of these failures as they affect systems, and the total effect of these failures and the interactions which arise, on the aircraft as a whole. In a presentation of this sort it is difficult to describe the complete procedure with greater depth but it is not difficult to see a direct parallel with the Failure Mode and Effects Analysis combined with Criticality Analyses which are performed in the US industry.

In a previous paper on the subject of safety assessment dealing specifically with Concorde (Ref: 1) the way in which these middle level assessments are combined was discussed. Essentially, we have designated a basic system element (Figure 1) which has an input of system control signals, stimuli from other systems, system internal failures and, of course, the system output functions. Within this concept it is endeavoured to have discrete analysis but the output of the analysis will be grouped in so far as their effects on the whole aircraft are concerned. A feature of each of these analyses is the use of dependence diagrams which make very important contributions to the achievement of total visualisation of system vulnerability.

The problem of display and total comprehension of the safety assessment introduces us to the question of choice between fault tree, logic tree, success path, dependence diagram, etc. I have had many discussions in the American and European industries where this has arisen and it is clear that there are applications and objectives which are suited to each approach. Bearing in mind the need to ensure that every section of the design/manufacturing/operating team should have the widest

understanding of the safety problem, it is suggested that some care should be taken over this choice. If the fault tree is considered it is thought that some variant, such as the logic tree, is very suitable as a high level linking discipline. It could link, for example, the outputs from the discrete system analysis referred to above and its use should be limited to the integration of these effects at the total aircraft level. It is suggested therefore that the roots of the fault tree should culminate in events which are described in dependence diagrams.

It is undeniable that pure fault tree analyses carried out with a view to automation are ideally suited to projects where development and operational time in a fully assembled mode is minimal. The fault tree programme in this case has some relationship to the flight development programme on aircraft but it is thought that from the point of view of original safety assessment on aircraft projects it is extremely difficult to highlight the safety problem, when a fault tree perhaps of many thousand events may be needed to go from a part failure to, for example, a minimum safe pitch capability over a limited Mach range. It is realised that statistical analysis will produce dominant paths, critical modes, etc. but it is possible that the complexity of the process could swamp the safety effort.

The dependence diagram is ideally suited to the examination of failure modes at system level and draws particular attention to the need for redundancy and the weight which must be put on the assessment. Attention is particularly drawn to systems which are unduly sensitive to series effects.

4.4 The Zonal Analysis

This is an analysis which is required to cover proximity, environmental and other associated effects which together constitute a considerable problem in most aerospace applications. A zone for the purposes of this paper is considered to be a volume or compartment of the aircraft which is structurally or even arbitrarily bounded and in which equipment and systems are installed. Convenient means of identification could be by the use of the ATA 100 coding suitably modified according to the specific structural requirements of the aircraft.

Zonal analysis could be considered to be primarily concerned with problems which arise as a function of position whereas the system analysis discussed elsewhere in this paper is primarily directed at failure to achieve Significant Airworthiness Functions. 'Primarily' is a key word in this context since there is an essential overlap and the dual approach is important. Zonal analysis would therefore be primarily directed at problems of containment, jamming, fire, leakage, radio interference, etc. These are essentially areas which require an adherence to design rules in respect of environment and segregation which can often be enshrined in arbitrary airworthiness requirements, and which have been developed with continuing experience over the years.

A systematic approach is required when the assessment is being made in the context of the rational requirement but the task of quantifying segregation for example is clearly a difficult one. The following method has been proposed for the use on current projects. The chosen zone must be identified in relation to the aircraft and its contents indicated by drawing or list. Installation rules are developed for each zone based on general experience, consideration of the particular equipment present, and its failure modes. The objective is to ensure compliance with the installation rules with reference to the hazard classification of the general requirement. If there is a case where the assessed hazard probability is not favourably matched to its effects then this will appear as an output of the Zonal Analysis. Apart from the direct environmental effect which would require local design action this hazard

would appear as an input to the safety analyses of the functional systems which are present in the zone insofar as the achievement of the associated Significant Airworthiness Functions are concerned.

It is worth repeating the primary features of this analysis which are to achieve a logical arrangement of the zones, clear identification of the contents of these zones, and the presentation of comprehensive installation rules. These installation rules must take account not only of the best engineering practice but also consider the specific failure modes and their local effects. Finally the zones must be comprehensively checked against these rules and positive conclusions reached.

5 THE EXERCISE OF JUDGEMENT IN SAFETY ASSESSMENT

Assessed probabilities are the essential tools of safety analysis and it is important that this statement is fully understood. In many cases it is possible to assemble an ideal structure of numerical probabilities on the basis of component failure rates. Particularly this is so in the case of avionics which are specially suited to statistical analysis on this basis and where substantiated failure rates for most of the parts and techniques involved are available. However, when safety assessment is being performed in this manner utilising component failure rates, weighting factors must be applied, to take account of particular usage, environmental conditions, etc. Therefore, even in what could be postulated as an ideal application of safety assessment where substantiated failure rates under known conditions are available, it becomes necessary to introduce general, if not subjective, experience into this numerical analysis when the required operating conditions are different from those under which the reliabilities were determined. The apparent derogation of a potentially 'pure' numerical analysis has been emphasised because the weighted analysis represents a point on the scale between 'numerical approach' on the one hand and 'engineering experience' on the other. Where the range of systems concerned extend from the purely electronic, through auto-throttles with, for example, sensors and clutch mechanisms, to flying controls where linkages, actuators, structural parts, etc. should also be included then it is obvious that the mixture has progressively become less 'pure'.

The 'pure' approach would be severely compromised when the interface between electronic parts and mechanical parts occurs, where one element has been assessed by proved reliability techniques and the other, such as a linkage or hydraulic component, may have been assessed on engineering experience associated with a limited but fully understood test programme. In cases of this sort, the failure of a mechanical locking device and a soldered joint in a circuit may have similar results.

So how should the task be approached? It must be emphasised that, as was said earlier, we are discussing only the tools of the trade; the designers and specialists have the desired input and it is the management of this input that is being discussed. Where computer techniques are required then the skills appropriate to these techniques must be available but only to ensure that the best use is being made of engineering judgement or the other relevant skills.

It is thought that a numerical approach is an excellent method of recording the exercise of judgement and it is emphasised that this should not be unnecessarily inhibited by the limitations of the data. The designer makes his numerical assessment implicitly by presenting his design and it can only do good to display how his thought processes have distributed the probabilities. The application of experience becomes more credible if directed at the component parts rather than at the assembly as a whole, and the design can be assessed by the extent of this dependence on unduly favourable assumptions. However it must be said that even here judgement must be exercised.

Unimaginative use of the numerical approach has tended to bring it into disrepute in some quarters and single faults estimated at 10^{-6} or less which produce dangerous hazards cannot be treated as the cornerstones of safety assessment. To avoid this

pitfall, rational requirements need to be backed by some safeguards stated in arbitrary form, as in TSS 1-1.

6 CONCLUSIONS

It is important to say before concluding, that there are major omissions in this paper, considered necessary because of possible effects on emphasis, within the limited time available. For example, safety assessments require major inputs from consideration of Crew Procedures; flight handling is closely linked with system analysis and rational requirements have been developed to take account of this; also no mention has been made of the importance attached to the use of the flight simulator and the importance of the continuing maintenance effort has only been mentioned indirectly. More specifically the analysis of digital systems (including their software) if employed where sufficient authority exists to create serious hazards is also relevant to the discussion of the fundamentals of Safety Assessment.

I think these examples suggest the extent of the field from which my particular observations could have been drawn. However I have chosen to bring out some of the essential features of Safety Assessment in more fundamental terms, which could have been obscured by these other considerations.

I have endeavoured to discuss Safety Assessment under four headings chosen at the beginning of this paper. I have talked about the definition of Safety Objectives, the organisation and display of the Assessment, and the exercise of judgement. I find that I have not specifically discussed the final point which was to show to the satisfaction of all concerned that the safety objectives have been met, and although it is largely implicit in the other headings, I will return to it later.

I think that the broad conclusion which emerges from this discussion is that Safety Assessment continues to require a disciplined approach, which, although it cannot displace the specialist design functions, is necessary as a means of directing these efforts at the right problems with a lower probability of subjective error.

In more detail, I have emphasised the need to determine and set out safety objectives with precision so that the analysis is not complicated, with occurrences which are not relevant to safety. Also it is important that the Safety Assessment can be readily understood by all concerned, and visual techniques such as the variants of the fault tree, dependence diagrams, should be used.

The exercise of judgement should be assisted where possible by a reasonable use of numerical methods, but these should not be allowed to obscure the objectives or saturate the Safety Effort. In addition, the particular importance of a methodical analysis of Zonal, or environmental problems, cannot be over-emphasised.

To return to the final point in my introduction which required the assessment to show to the satisfaction of all concerned that the safety objectives have been met, this is of course a problem of data display and management. If judgement has been applied in the manner discussed so that simulator, development flying, and service experience can rapidly and effectively update the assessment, then I believe that we are some way along the line towards ensuring that the Safety Objectives will be achieved in service.

7 ACKNOWLEDGEMENT

I would like to express my thanks to the Air Regulation Board for permission to present this paper and to point out that the opinions expressed are entirely my own.

8 REFERENCE

1. HAAS, J. (Aerospatiale), 'An Application of Modern Maintenance Concepts and Safety Analysis to the Multinational Certification of a Supersonic Aircraft.' Presentation to the 6th Annual International Maintenance Symposium.

APPENDIX

NOTE ON TSS 1-1 AIRWORTHINESS OBJECTIVES AND SYSTEM ANALYSIS

TSS 1-1 introduces a probability approach to the Safety Assessment of aircraft systems, together with a framework of defined terms. To fit the requirements into a consistent framework, a number of terms needed to be defined.

At root there are the things which happen, described as Occurrences. These include Failures of parts of the aeroplane, Events arising from outside the aeroplane (e.g. gusts) and Errors arising from the actions, or failures to act, of flight or ground personnel.

An Occurrence has various potential Effects. These can be classified according to the associated level of danger, into Minor, Major, Hazardous or Catastrophic.

The requirements must state the acceptable frequency of Occurrences, and according to the magnitude of the Effect, various frequencies can be ascribed - Frequent, Reasonably Probable, Remote, Extremely Remote, etc. To give technical significance to these words some idea of the numerical probability needs to be quoted (e.g. Reasonably Probable, of the order of 10^{-3} to 10^{-5}).

The constructor's task is then to assess the frequency of Occurrences, singly and in combinations, and the Effects of these Occurrences. These results are then to be matched against the acceptable probability of the various levels of Effect.

One clearly defined difficulty with this approach is that of proving compliance with the requirements, particularly in cases where a failure or combination of failures would result in catastrophe. In such cases it is necessary to impose some additional arbitrary criteria in addition to, or instead of the numerical criteria (e.g. a double failure may only be acceptable as an Extremely Improbable failure when (a) both failures are assessed to be not more probable than Remote, or (b) at least one is assessed to be Extremely Remote).

The requirement then states broadly that the Occurrence of failures or errors must not produce an accident risk greater than prescribed levels, and that systems or combinations of systems operating normally without failures or errors must not be able to able to prejudice the safe operation of the aircraft.

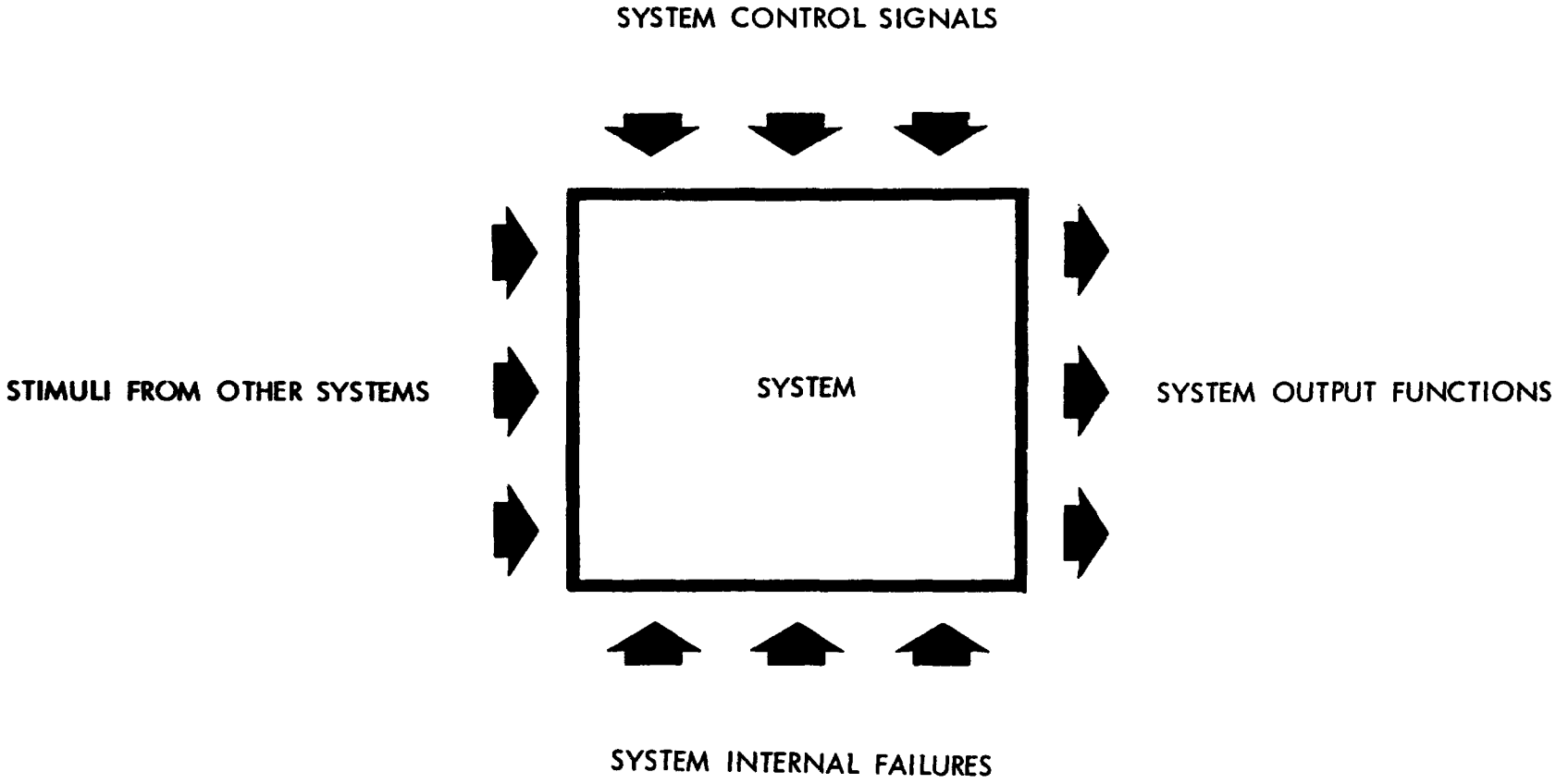


FIGURE 1 BASIC SYSTEM ELEMENT

PILOT SAFETY FOR THE X-24A LIFTING BODY VEHICLE

John Cochrane and Kenneth Graham

Martin Marietta Corporation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

The X-24A is a manned lifting body flight vehicle, engaged in a flight research program at Edwards Air Force Base, California. The aerodynamic configuration of the X-24A was developed by the Martin Marietta Corporation over a period of years in connection with in-house studies and Air Force contracts. The final configuration evolving from these studies was identified as the SV-5. The SV-5 configuration featured medium hypersonic lift to drag ratios, good subsonic performance, and a high volumetric efficiency.

Three small scale SV-5D vehicles, identified as the PRIME, were fabricated by Martin under Air Force contract. They successfully demonstrated flight from entry into the earth's atmosphere at orbital speeds down to 100,000 feet altitude at a velocity of Mach 2.0. The unmanned PRIME vehicles were approximately one fourth the size of the X-24A and weighed approximately 800 pounds. Recovery was by "air snatch" following deployment of a ballute and a parachute.

DESIGN AND OPERATIONAL CHARACTERISTICS

The X-24A is approximately 24 feet long, weighs approximately 5500 pounds empty, and has an internal tankage capacity for approximately 5500 pounds of propellants and gases. It is of conventional aluminum alloy construction and is powered by the XLR-11 rocket engine developed over twenty years ago. The main propellants are liquid oxygen and alcohol. Hydrogen peroxide is used to power the turbopump and helium is used to pressurize the tanks and actuate the valves. The vacuum thrust of the engine is approximately 8500 pounds and the maximum burn time at full thrust is nominally 140 seconds. 500 pound thrust hydrogen peroxide fueled rocket engines are also provided for use as "landing engines".

Control of the X-24A is by means of 8 movable aerodynamic surfaces. These surfaces are powered by a duel redundant hydraulic system and respond to either pilot commands or the inputs from a triple redundant stability augmentation system. Various modes of control are possible with the X-24A and the development of a "control law" has been one of the objectives of the flight research program. Generally the upper flaps are "biased" to the open position at high speeds (minus 40 degrees above 0.60 Mach number, for example) and are closed up at low speeds and for landing. The pilot has the capability, however, to open them up for use as speed brakes. Usually, pitch control is accomplished by simultaneous deflection of the lower flaps while roll control results from differential deflection. When the upper flaps are "closed up", some of the pitch and roll control functions are transferred to them at which time they act in concert with the lower flaps.

The upper and lower rudders on each side may be moved together in response to "bias" signals and are generally toed-in 10 degrees for low speeds and toed-out 2 degrees for high speeds. The upper rudders on each side move together in response to the pilots commands, inputs from the stability augmentation, and in response to commands from a rudder-aileron interconnect system. The rudder-aileron interconnect system deflects the rudders in proportion to aileron deflection to counteract the adverse yaw which results from aileron deflection. Aileron action is, of course, obtained by differential deflection of the flaps as explained above.

The normal mode of operation of the X-24A is to launch the vehicle from a B-52 mother ship at approximately 45,000 feet and a Mach number of 0.69. Early flights were made in a strictly glide mode. Later, the XLR-11 rocket engine was started after launch and the X-24A was climbed to altitudes in excess of 70,000 feet and accelerated to velocities in excess of Mach 1.60. In all cases, however, the final portion of the flight consists of an unpowered glide to a conventional airplane type landing on the dry lake at Edwards Air Force Base.

SAFETY CONSIDERATIONS FOR VEHICLE DESIGN

The "one of a kind" research mission of the X-24A dictated that great emphasis be placed on safety during the design of the X-24A. Initial criteria were developed on the basis of experience with other research flight vehicles such as the X-15 and on the basis of the predicted flight characteristics of the X-24A.

The inherently high drag of the lifting body configuration together with its relatively low lift/drag ratio (typically 2.0 to 4.4), generated considerable concern with respect to the pilot's ability to perform safe landings from gliding flight. Accordingly, the "landing engines" were incorporated into the design to provide an increase in the apparent lift/drag ratio during flare and landing. Experience with the X-24A has since shown that this concern was not warranted. The landing rockets were used on the first three flights, but have not been used on the following twenty-two flights.

In the early stages of design, all systems were reviewed for critical areas. A failure mode and effects analysis was performed. Redundancy and other techniques were used to insure safe operation to touchdown and roll out after one or more component failures occurred.

Start failure of the XLR-11 engine would require immediate jettisoning of the main propellant. Therefore, a bypass system was designed which would route helium directly from the storage tank to the main propellant tanks. An interlock with the jettison valves prevented opening of the bypass system unless the jettison valves were open. Thus, a failure of the normal pressure regulating system in the closed mode would not preclude jettisoning of the main propellants.

The hydrogen peroxide tank is pressurized with helium to 475 psia. The helium is stored at 4200 psia and routed through a pressure regulator to achieve the desired pressure drop. An open failure of the regulator would over pressurize the peroxide tank and cause a catastrophic failure. This single point failure was eliminated by incorporation of a dual redundant relief valve in the peroxide tank. Depletion of the helium source through the vent is prevented by installation of a normally open solenoid valve in series with the regulator. This valve is controlled by a pressure switch, set to a higher pressure than the regulator pressure, but a lower value than the settings on the peroxide tank relief valves. A cockpit switch allows the pilot to close this valve manually if his pressure indications should show a trend to over pressure, or to de-energize the valve if a pressure switch malfunction should cause it to close unnecessarily.

Redundancy techniques were used in the flight control system to eliminate single point catastrophic failure modes. Two independent hydraulic systems are used. Each system is powered by two electric motor driven hydraulic pumps, and each pair of pumps is powered by its own independent battery. In the event of a failure of either of the batteries powering the hydraulic pumps, power is switched to the flight test instrumentation battery, thus providing an additional backup for this mode. The stability augmentation system was made triple redundant to insure that it would always be available to provide its augmentation function, but could not command a "hard-over" or other erroneous control signal. Each axis of the system has three parallel rate gyros, associated electronics, and a logic circuit which insures that a malfunction in one of the three parallel channels will not cause a hardover or disable the system.

The X-24A flight control system consists of a relatively complex mechanical linkage which accomplishes the required mixing and crossover functions in order to transfer the command signals from the pilot and the stability augmentation system to the flaps and rudders.

In order to thoroughly evaluate the operation of the flight control system under normal and malfunction conditions and to accomplish the necessary development work in an orderly and expeditious manner, the entire system was assembled on a structural steel mockup for fixed-base closed loop simulation. All attachment points to the basic X-24A structure were duplicated by the structural steel frame work. The hydraulic power actuators moved dummy control surfaces which were loaded in a manner to simulate airloads. This was accomplished with air cylinders pressurized from a regulated source of compressed gas. Control surfaces position was measured with potentiometers and the electrical signal was fed into an analog computer. A complete set of pilot flight controls was provided and the position of these controls was also fed into the computer. The motions of the X-24A which would have resulted from the various control positions was calculated by the computer and displayed on the pilot's flight instruments (attitude indicator, Machmeter, altimeter, etc) and also recorded

on strip charts for engineering analysis.

Experienced pilots "flew" numerous missions in both normal and malfunction modes. These tests provided functional verification of overall system operation and permitted an assessment of the pilot's ability to use the manual backup controls to correct system malfunctions. A typical example would be a failure in the automatic flap bias system tending to drive the upper flaps to an extreme position. The pilot was able to switch to the manual mode and "beep" the flap to the desired position before the development of a serious situation.

After delivery of the X-24A to the government, gull scale wind tunnel tests were run in the large low speed tunnel at the Ames Research Center. Additional small scale tests were run, and this data together with the measured characteristics of the actual X-24A flight control system were used to develop an accurate simulation program. This simulation did not include the actual flight control systems hardware as in the flight controls test stand described above. Instead the measured characteristics of the flight control system were programmed into the computer. This simulator provided an accurate duplication of the cockpit controls and displays and the computer output drove both the pilot's displays and an X-Y plotter similar to the one used to control actual flights.

OPERATIONAL SAFETY

Flight planning for the X-24A starts with a review of all available data from preceding flights and a comparison of this data with wind tunnel results. A configuration (control settings, gains, etc) is established for the flight together with a set of flight objectives. In general, the flight objectives are to obtain specific data under certain flight conditions (Mach number, angle of attack, etc). Flight planning for a vehicle such as the X-24A must consider many factors in attempting to accomplish the desired flight objectives. Energy must be programmed to insure that the primary landing site will be reached with sufficient speed and altitude to insure a safe landing, but provisions must also be made for abnormal situations such as an early engine shutdown. The simulator is used as a tool for planning the nominal trajectory as well as all malfunction situations. In addition, it is used as a means of evaluating changes to the flight control system or other ships systems relative to their effect on stability and control and performance.

Once a satisfactory flight plan has been developed, the simulator is used for crew training. The general procedure used in the lifting body flight test program has been to have at least two pilots specifically assigned to one of the flight vehicles and at least three pilots active in the program. One of the X-24A pilots is assigned to fly the mission and the other pilot is assigned as the controller (NASA One). Usually, the third pilot, although not specifically assigned to the X-24A, will fly chase. The flight planner, the controller (NASA One), and the mission pilot use the simulator to train for the mission as a team.

As a further training aid, F-104 aircraft are used as airborne simulators for the approach and landing phases of the mission. Aerodynamic data for the X-24A and for the F-104 are utilized to establish an F-104 configuration which will give it lift/drag ratios comparable to that anticipated for the X-24A in the upcoming mission. Typically, the F-104 is flown with gear and flaps down, speed brakes extended, and engine at minimal power settings to duplicate the low lift/drag ratio of the lifting body. Practice approaches are flown for the normal mission and for all of the malfunction cases. On the morning before the flight, a final set of practice approaches are flown, usually with the chase pilot accompanying. Thus, when the mission pilot embarks on the actual X-24A mission, all normal and emergency aspects of the mission have been experienced and he is thoroughly prepared for any foreseeable situation which might develop.

A further safety procedure followed in the development of an X-24A mission involves preparation of the formal written flight plan, and the technical and crew briefings. The flight plan spells out in detail all aspects of the flight. Each event in the flight is detailed in terms of Mach number, altitude, angle of attack, elapsed time, and maneuver to be accomplished. A set of ground rules for "no

launch" and a set of alternate situations after launch are defined in detail.

Several days before the scheduled day, a technical briefing is held. This briefing is attended by all cognizant personnel from both NASA Flight Research Center and the Air Force Flight Test Center. Data from the preceding flight are reviewed and the technical aspects of the upcoming flight are discussed in detail. Finally, the written flight plan is reviewed. All questions raised at this briefing are answered satisfactorily as a prerequisite of the flight.

The crew briefing is accomplished during the afternoon preceding the scheduled flight day. This briefing is attended by all personnel who will participate in the actual accomplishment of the flight. All operational aspects are reviewed and the personnel assigned to accomplish specific tasks are identified. Any special operating procedures are discussed and the chase pilots, B-52 mother ship pilots, airborne photographers, and mission pilot coordinate their activities at this time.

Servicing of the X-24A begins approximately two hours prior to pilot entry into the cockpit. A complete controls system check is accomplished during this time period. "Throwboards" are attached to the X-24A to measure control surface deflections. An observer is stationed in a position to make the desired readings. The crew chief operates the controls in the X-24A cockpit and a controls engineer directs the test from the control room. The X-24A telemetry system is operative and driving the strip recorders which display control positions in the control room. All personnel participating in the test are in radio and/or telephone communication. The test verifies that the control surfaces are in fact properly responding to the pilots cockpit control motions and that the control room recorders are displaying the actual positions of the control surfaces. This check also verifies proper operation of the stability augmentation system and the automatic bias system.

Approximately 30 minutes prior to pilot cockpit entry, the pilot is prepared for flight. A special van located near the X-24A is utilized to instrument the pilot and fit him into his full pressure suit. Since powered flights of the X-24A are normally made to altitudes in excess of 50,000 feet, the pilot wears a full pressure suit as a backup in the event of cabin pressurization failure. In order to obtain biomedical data, the pilot is instrumented with special sensors, the output of which are recorded on a small tape recorder. A flight surgeon is present during all preparation of the pilot for flight to provide medical aid in the event of an accident, and to observe the pilot for any signs of distress. This procedure was instituted when a lifting body pilot suffered severe dehydration due to the high ambient temperatures (Edwards Air Force Base in the summer) encountered during a hold which occurred after cockpit entry.

After pilot entry into the cockpit, the X-24A crew chief and the chief inspector go over the "pilot entry checklist" with the pilot to verify the position of all cockpit controls and the reading of the appropriate displays. The entire captive portion of the flight is also conducted in accordance with a carefully prepared checklist i.e. countdown.

Timing of the checklist during captive flight is a function of B-52 position and is arranged so that completion of the checklist occurs just as the B-52 approaches the launch point. During the captive portion of the flight, another complete controls system check is accomplished. This check verifies proper operation of the system in the actual flight environment. In addition, pitch and yaw pulses of the B-52 permit an operational check of the stability augmentation system. Air for cabin pressurization, breathing oxygen, and electric power for the X-24A are provided from the B-52 until approximately five minutes before launch. At that time a switchover is made to internal systems and a check is made to determine that operation is satisfactory.

Upon reaching the launch point, the pilot launches himself and proceeds with the flight according to plan. The flight is monitored from the ground and all communications with the pilot are filtered through the controller (NASA One). The pilot is advised of any malfunction or abnormality and provided with recommended corrective action. His trajectory is monitored from the radar driven X-Y plot and heading and climb angle corrections are provided as required. During the approach, the chase pilot flies in close proximity to the

X-24A and provides airspeed, altitude, and turbulence information. In addition, the chase pilot verifies satisfactory extension of the landing gear and advises the pilot of his height above the runway during the last 100 feet of descent. Normally, the chase aircraft touches down in formation with the X-24A. The entire operation is one in which teamwork and thorough training play a very important part. By means of these procedures, flight testing of advanced, radically configured experimental flight vehicles is conducted in a very safe manner on an almost routine basis.

CONCLUSION

The lifting body flight test program has been conducted on an extremely austere basis. The entire cost to the government of the X-24A program, including vehicle acquisition, has been less than the cost of many paper studies. Yet, there has been no compromise with safety. Safe operation of such a radical flight vehicle has required careful attention to safety considerations from the beginning of the design process, and with continued emphasis right through the flight program.

SESSION II

QUESTIONS AND ANSWERS

QUESTION: John, where do we go from here in manned lifting bodies? Is the space shuttle next or is there something in between?

MR. COCHRANE: The present plan is to modify the X-24A to a new configuration known as the X-24B which has higher hypersonic performance. It will be a sort of long skinny vehicle instead of a short fat one but it is the same basic core. We will actually add the structure to this vehicle and retain the systems, that is anticipated to be done sometime late this year. Then, a lot of us at NASA are hoping that we will have a similar type vehicle to represent one of the space shuttle orbiters or boosters perhaps. I think the booster is the one that they are thinking of presently.

QUESTION: What is the thrust in the "B"?

MR. COCHRANE: It will be the same thrust. The engine will be the same and the engine does develop 8500 lbs. of vacuum thrust.

COMMENT: You mean the engine is still good, we are going to use it many more years, right John?

MR. COCHRANE: Yes sir, I might comment that the present thinking is to use two of them. This would give us eight chambers in the drop vehicles, that is the shuttle vehicle--space scale shuttle, and I shutter to think of getting eight of them going. Yesterday we sure had a lot of trouble getting four going.

QUESTION: Did you use any techniques of system safety discipline on the X-24A or did you just design in good safety features.

MR. COCHRANE: I would say yes, but I have to qualify it. I deliberately did not get into a discussion of it because I didn't have time. I think what it was, the technical director on our program had been a reliability engineer previously and the techniques were not the formal techniques that have been discussed here earlier, that is with charts and procedures, etc., but it was a case of, I think individual responsibility, people who had worked in the area and who were very aware of it. I don't know if that answers your questions.

MR. GORDON SMITH/A.F. SYSTEMS COMMAND: Mr. Hammer -- Willie, I know you made a number of comments about changes that are needed in MIL-STD-882. I was wondering whether you have already submitted these officially for consideration or whether you are going to submit them?

MR. HAMMER: No I haven't submitted them officially at all. As a matter of fact, it was only Thursday or Friday that I heard the Air Force was actually thinking of revising MIL-STD-882. Lets say I presented a few comments, I even have a few that I did not put up here because I didn't think that they were that important. If you want Gordon, I can just get you a copy and hand them to you.

MR. SMITH: The best thing Willie is to submit them on that form that is in the back of the MIL-STD. When we went through the last exercise we got recommended changes on wrapping paper and everything else and we had one heck of a time. We are hoping in this current revision of 882 to stick to the format of the form that is in the back of each copy of the MIL-STD, then we have them in apple-pie order and we can give them due consideration. There is one other advantage of using that form, with the high postage rates, the way they are, we pay the postage on that form.

QUESTION: Mr. Hammer you made a couple of statements on MIL-STD-882. One that you would prefer not to see a categorization. As a nuclear system analyst, I'd like to know, when we do analysis what could we use to categorize?

MR. HAMMER: Why do we need categorization. This is what I want to point out, that if the procuring activity or the agency that is interested in getting a system developed actually indicates where the investigations, which way the safety activities should go, you really don't need these safety

categories. Actually, the old idea about the categories was the fact that if they said, well if you have a Category IV then you know it is more important than Category III, II, or I. This was the benefit of the four categories. As I say, I think that we have advanced so far now that we really don't need the categories, that whoever is responsible for obtaining a new system could actually stipulate the various problems that they want investigated. In some of the work that I have done with various organization, I found it is a great deal of trouble trying to decide which of the categories these things go into. For example, lets point out this deal about injuries. You have two categories for injury, Category III and Category IV and it is quite a problem trying to determine, if the person who is going to over here going to be subjected to a Category III hazard or is he liable to be killed and be in a Category IV hazard. So as I say then, other things are these delineations between the categories. For example, Category IV talks about system loss; Category III talks about the fact that you might lose the system unless immediate corrective action is taken. Which means that you have a potential for system loss in the Category III hazard, so which do you put it under, Category III and IV. The other point is that we sometimes get the question do you put somethings in Category I, II, III or IV depending on something like the probabilities that Mr. Allison had. Whether it is highly improbable, very low probability of hazard, or do you take anything of any probability and put it in a category and just leave it there?

VOICE: I understand your point but the other one I think we are all interested in, is why is it 180^{0} out of phase with the reliability category.

MR. HAMMER: I hate to say this but I believe that when 38.30 was developed the military specification at that time had four reliability categories. I think they figured if reliability had categories, safety ought to have categories and just to differentiate the two they ran them in opposite directions.

VOICE: Since the speaker asked a question why categories, I guess some of the audience can answer the question. I think the categories were just a stepping stone to management action. For instance in configuration management you'll have a Level I review board, Level II Board, Level III - and when you assign a design change it establishes the level which review and decision can be made. I think there was an implication that Category IV would have to be reviewed as a high level of management; Category III as a low level of management, etc. Unless the management system goes on and says that unless the management system identifies some correlation between the responsibility and authority for disposing of the hazard, then the Category itself is meaningless.

MR. HAMMER: Categories have this one basic advantage, the fact that supposedly you look at the Category IV and you say, we want to pay more attention to that, but we get involved with another problem in determining the categories. For example, taking a missile that we are trying to establish categories on.

Say this is an air launch missile. We know that if the electrical system fails on a missile that has been launched that you have system loss. System loss is Category IV. Now, you can have an electrical system failure for a number of reasons. One of the reasons is that you lose the battery which means that if the battery fails then you have a Category IV hazard. As you go down you begin to analyze what could cause the problems within the batteries and you can have sixteen different items such as touching plates, a poor connection, poor soddering, each one of these things. Does that mean that poor soddering within the battery is a Category IV hazard because you are ultimately going to lose the system. Now you have to have a Philadelphia lawyer to begin to figure out where do you stop categorizing these things as Category IV or Category III. This is not well-defined in MIL-STD 882.

QUESTION: Again for Mr. Hammer, the point of categorization. The categorizing system sure is simply a means of shorthand, I agree that it has serious problems. Perhaps it needs expansion rather than eradication. For example one serious injury or a thousand deaths would both be a Category IV hazard when you can hardly compare the two in any system safety program. That is simply an aside. My question really is that MIL-STD-882 says in about 5900 words exactly what 38-130A

said in 2500 words. Is it your opinion that 882 is a step forward? a step backward? or a step sideways in comparison to 38-130?

MR. HAMMER: I think the chief advantage in MIL-STD-882 was in the delineation of the tasks and the various phases. Here again, I think certain of these items should be improved. For example this deal about the system safety program plan, both in 38-139 and MIL-STD-882. In the conceptual phase they have no requirement for the system safety program plan. The system safety program plan actually comes into being in the Phase A definition. I know that lately they started changing the various phases, but it comes into the Phase A definition and it is actually prepared at that time for use during the Phase B and for the engineering phase which means that the system safety program plan according to 882 is not prepared for use during the current work being done on a system. In actuality most of the procuring activities require that a system program plan be prepared and that is actually used during the current phase but it isn't what this says in MIL-STD-882. As I say the big advantage, to answer your question of 882 over 38-130 was the delineation of the safety tasks.

MR. RUSSELL (GE): I have been spending about the last two years working with a chemical and petroleum industry and applying some of these techniques and I would just like to pass on for the benefit of this conference that they continually remind me that a lot of industries are not like NASA and aerospace in terms of dollar resources. Unless I can show them a series of category definitions by which they can decide who can work on these problems and how many dollars that the line manager, as Mr. Pope so adequately pointed out, can be allowed to address this problem with, they are not very much interested in using NASA and Aerospace techniques in their current dilemma with the environment.

MR. HAMMER: I point out the fact that one of the biggest problems we actually have in management is trying to understand some of this differentiation between reliability and system safety. I have seen statements of work that say "failure mode analysis will be conducted." Now safety goes beyond that.

It is not only failures, you have the environment effect, you have personnel errors, you have a lot of other things that actually the reliability people did not consider and so in writing the statement of work, where it is the statement of work again it is necessary that they be clear in making sure this is a safety effort and not a part of a reliability effort. I might say that June 10th, Machine Design is going to have another article and it is going to be on reliability versus safety as related to liability. In this we point out the fact that indicating in warranties that an express warranty, where you say a thing will last a certain length of time, 50,000 miles or 5 years, is actually a warranty that relates to reliability. The implied warranty that a product must be safe if it has no time limit actually on the thing is really the system safety aspect of a liability suit. In addition to that I try to point out, the article was cut down, was the fact that if you have an accident and a liability suit arises, it doesn't matter what the test reliability or the operational reliability or the design reliability was, you can be sued for negligence in design and a lot of other things unless you have taken suitable safety action. There is a great difference between the reliability and the system safety but frequently, as I stated before, the expressions in the statement of work do not reflect. We then have trouble with management in trying to indicate that there is a difference.

SESSION III

SYSTEM SAFETY EDUCATION

Session Chairman - Mr. Vernon L. Grose

"System Safety Education Focused on Flight Safety"	Mr. Eugene Holt
"System Safety Education Focused on Industrial Engineering"	Dr. W. L. Johnston
"System Safety Education Focused on System Management"	Mr. Vernon L. Grose

Opening Remarks for Session III

SYSTEM SAFETY EDUCATION

Vernon L. Grose, Session Chairman
Vice President
Tustin Institute of Technology
Santa Barbara, California

When I was a boy, our daily newspaper regularly carried a cartoon with the caption, "Heroes are born-- not made." Those of us in the field of system safety today have arrived there from an amazingly diverse set of backgrounds. As so-called "charter members" of this discipline, we could be considered the "heroes" of system safety. Many of these heroes are convinced that they know all there is to know about the subject. In fact, some may feel that they invented system safety!

To those not quite so self-assured or those yet possessing some humility regarding their mastery of the subject, this session on System Safety is dedicated. We believe that education of a formal variety is not only a nice idea but a vital necessity if system safety is to become and remain a truly professional activity.

So if you were not born a hero of system safety, we propose that you can be made a hero-- even at this late date-- through education.

Every great idea is said to have its own time of arrival on the scene of history. Breakthroughs in medicine, aeronautics, economics and other fields are often achieved simultaneously in widely-separated areas of the world without collaboration. A current example of this precept is the marked similarity in appearance, size, and performance between the Soviet Union's TU-144 and the Anglo-French "Concorde" SST.

The speakers in this session will illustrate the thesis that "system safety's time has now arrived." To further reinforce this thesis, you will note that the subjects discussed in this session all have a different root or source for system safety education, and the educational institutions represented are separated by at least 1000 miles!

The first paper discusses system safety education as it emanated from a world-renowned base of aviation safety at the University of Southern California. The Institute of Aerospace Safety, which dates to 1952, provided a unique foundation for system safety education.

The second paper depicts system safety education spontaneously arising in the Industrial Engineering Department at Texas A&M University where similar courses in maintainability engineering and production design engineering had been also offered for several years.

The third and final paper provides yet another phylogenesis for system safety education-- the field of system management. The George Washington University School of Engineering and Applied Science conceived their system safety course as a natural outgrowth of the systems approach to management.

We had intended to have a fourth university represented on the program today-- the University of Washington. To that end, I had requested that Professor Berl W. Owens, UW's System Safety Course Coordinator, prepare a paper entitled, "System Safety Education Focused on Quantitative Techniques." His course, dating from 1965, is well-known for its specialization on Fault Tree Analysis and has been attended by perhaps more personnel than any of the three courses being discussed in this session today. In a letter dated 9 March 1971, Professor Owens wrote to me:

> ". . . Thank you very much for the opportunity to present a short paper and present it before the Government-Industry System Safety Conference on 26-28 May 1971. It is indeed a top level conference and I am sorry I must decline. I am in poor health at the moment and cannot get away from home..."

I am grieved to report to this Conference that approximately two weeks ago, Professor Owens passed away in Seattle. In his honor, I request that we stand for a moment of silence. (The Conference thereby honored Professor Owen's memory.)

The contrast between origins for system safety education is most interesting. Because this session is designed to reinforce the Conference theme-- "to broaden the application of system safety into many areas outside aerospace," consider the breadth of education to be discussed today:

1. All three courses discussed are of different length or duration.
2. Some of the courses are offered for college credit, others are not.
3. The courses are offered on the East Coast, West Coast, and the Great Southwest.

SYSTEM SAFETY EDUCATION FOCUSED ON FLIGHT SAFETY

Eugene Holt
University of Southern California

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

General John D. Ryan, Chief of Staff, United States Air Force, in his keynote address at the 1969 Air Force Industry System Safety Conference, made a significant statement concerning System Safety. General Ryan stated, "We have encouragement by our competence in the engineering disciplines, but. . .many of our deficiencies in safety can be traced to a prevalent flaw, not in the area of competence, but in attitude." The problem identified by General Ryan is of particular significance in the field of System Safety. Many of our deficiencies in system design could be eliminated with proper attention and early attention to the "demands" of safety. However, the "demands" of safety in many cases are not adequately considered as a result of a negative safety attitude held by non-safety personnel in decision-making positions. This basic attitude toward safety results in the feeling that safety in general and safety programs in particular will inhibit or restrict or otherwise limit operations. The resultant atmosphere finds the system safety engineer in a defensive position attempting to convince personnel who, in the first place, are probably not technically qualified, and secondly, do not understand the system safety concept; in short, ultimately making the "hard sell" to a person who is not buying. Objectivity dictates that these management and non-safety personnel are normally influenced by the pressure of schedule constraints, budget limitations, and performance-oriented design groups. The realization that these personnel are also influenced by a sometimes unconscious bias or negative attitude in reference to the general subject of safety, let alone the lesser understood discipline of System Safety, should serve as a cause for great concern among safety educators. For as we ponder this situation and begin to evaluate proposed solutions to the problem, which incidentally is no unique problem and does not have a unique solution, the answer continues to come up SYSTEM SAFETY EDUCATION. We must educate until management and non-safety personnel recognize where and how utilization of the system safety process can best serve their needs.

The faculty and staff of the Institute of Aerospace Safety and Management, University of Southern California, are dedicated to the proposition that basic safety education is of fundamental importance to the success of accident prevention programs. The Institute, presently in its nineteenth year of operation, consists of two divisions and a Research Center. The Safety Division, founded in 1952, offers a variety of safety education programs designed as short courses which vary from one to twelve weeks in length. More than 9,000 students have attended Safety Division safety courses including personnel from the aerospace industry, commercial aviation, general aviation, the United States Armed Forces, and students from foreign countries. Notable alumni include astronauts Alan Bean, James Lovell, Jr., and Walter Schirra and the 1969 Harmon Trophy winner Major Jerry Gentry. The Graduate Division, founded in 1963, offers a graduate degree program, Master of Science in Systems Management. Operating from 26 graduate study centers located around the world, more than 1,775 master's degrees have been conferred. The recently established Research Center concentrates on research and development in flight safety, highway safety, transportation systems, and human factors.

SYSTEM SAFETY EDUCATION

The Institute of Aerospace Safety and Management has developed and conducted many different types of safety courses. In fact during the last fiscal year, 45 separate courses representing different programs were presented. These courses include Aerospace Engineering, Missile Propulsion Systems, Aircraft Accident Investigation and Prevention, Communicative Skills in Safety Education, Aviation Psychology, Aerospace Physiology, Aerospace Safety Management, etc. Although the major emphasis in all of the courses is safety, four of the courses deserve special attention in this paper due to their relevance to the subjects of Flight Safety and System Safety. These courses are:

I. Flying Safety Officer Course
II. Advanced Safety Program Management Course

III. Fundamentals of System Safety
IV. Quantitative Methods of Safety Analysis

- - - - -

I. The Flying Safety Officer (FSO) Course is presented to rated pilots of the United States Air Force and Air National Guard who are assigned to Flight Safety or Safety Staff Officer duties. The initial FSO course began 16 March 1953 and since that time 90 courses involving some 2,300 students have been completed. The FSO course is designed to develop in the student an understanding of the principles of accident prevention and how to incorporate these principles in an accident prevention program, an understanding of current flight safety educational methods in the Air Force, the ability to recognize hazards involving human performance, equipment performance, physical environment, and the interrelationship of these hazards, knowledge and skill in the supervision of aircraft accident investigation, an understanding of accepted principles of learning and the ability to apply them to instructional situations, etc. No specific reference to the subject of System Safety has been made; in fact, only recently have system safety engineering techniques and a general discussion of the System Safety concept been formally introduced into the FSO course curriculum. Rather the FSO course has been singled out here because of its fundamental importance and great tradition in safety education at the University of Southern California. System safety education at USC has its very roots in flight safety. Flying safety is concerned with the recognition, prevention, and elimination of all hazards to flight and the flying safety officer's job is primarily educational. He must assure that hazards are known and understood with an awareness of required corrective actions. Comparable course are also presented to U.S. Air Force Missile Safety Officers and U.S. Army Aviation Safety Officers.

II. The Advanced Safety Program Management (ASPM) Course provides specialized safety education for officers of the U.S. Air Force and civilians, GS-11 or higher, in order to assist in their further qualification as Safety Staff Officers. The initial ASPM Course began in November, 1964, and since that time 20 courses involving more than 500 students have been completed. The ASPM course is designed to develop in the student an understanding of the principles of management and the relationship of these principles to the management of effective safety programs, the basic principles of safety required for the development of a philosophy of safety, the collection, preparation and analysis of source accident data, the basic principles of motor vehicle safety, and an understanding of communications and industrial relations in safety management. The instructional material on the collection and analysis of accident data has recently been expanded to include not only the traditional methods of post-accident data analysis but also what has been termed pre-accident investigation. The instructional section begins with the graphical presentation of accident data, the derivation of accident rates, basic probability theory, statistical safety measures, confidence and risk, and the utilization of accident data in safety decision-making. System safety education has thus been introduced as a fundamental approach to accident prevention which is more effective, ensures greater leverage in design analysis and decision-making, and also affords the most economical approach to preventing accidents. Graduates of the ASPM course, who receive seven units of graduate credit, usually have a basic understanding of and practical experience in flight safety. Inclusion of system safety education in the curriculum has allowed these students' basic understanding and philosophy of safety to evolve and expand toward more of a total safety concept, including system safety and operational safety as an integrated approach to accident prevention.

III. The course, Fundamentals of System Safety, presents a curriculum of system safety education in its truest sense. The initial System Safety course began in October, 1963, and since that time 18 courses involving over 400 students have been completed. Prerequisite for this course is a bachelor's degree, preferably in an engineering or technical field, or three years of safety, system engineering, or maintenance experience. Three units of graduate level credit are given for satisfactory completion of the three week course.

System Safety as a fundamental approach to accident prevention has been and is continuing to be a rapidly expanding field which requires the best managerial and technical talents available. System safety educational programs have consequently been required to remain flexible in meeting the challenges of this expanding new discipline of System Safety. At the University of Southern California minor System Safety Course modifications have been made with almost every class. In fact, several major curriculum changes have been required during the past five years. It is believed that the experience gained through such a course evolution will prove critically important to the future success of system safety education at U.S.C.

The primary mission of the present System Safety Course is to develop within the student a basic understanding of the total system safety concept. The course is designed to address both the management and the engineering aspects of System Safety. The presentation of management and engineering material in a proper balance is both delicate and critical. Further, while the term System Safety properly defines a program to cover the entire life cycle of a system, the primary interest should be directed to the concept, definition, and development or so-called "design" phase of the system's life. System Safety will thus complement the established traditional safety efforts during the operational phases of a system. A system safety educational program should, therefore, be directed primarily to the earlier design phases of system life, devoting enough attention to the later operational phases to allow the student to understand the total scope of the system safety effort. The system safety engineering methods which may be applied during the design phase to evaluate the relative safety of proposed system designs are not only more technical and penetrating, but more quantitative also. The system safety engineering portion of the course should prepare the student to both perform and evaluate the vital safety analytical function; namely, the identification and control of system hazards. The system safety management portion of the course should familiarize the student with the planning, organizing, directing, and controlling aspects of management.

During the development and presentation of the instructional material of the course, the U.S.C. faculty have reviewed current industry and government system safety technology, adapted basic principles and specific methodology to individual aerospace applications, and genuinely pursued a course which is more than another theoretical discourse. Selected guest lecturers from industry enrich course content with "real world" experience. An extremely effective class group project, recently instituted, has proven successful in preparing the students for necessary System Safety program planning, organizing, job descriptions, and costing. A unique and beneficial aspect of the class group project is the coordination required of military and civilian students as team members. Working together on a team a common goal promotes a better understanding of the problems that each must face respectively.

A similar course is presented to Department of the Navy safety personnel in the Washington, D.C. area, except that separate system safety management and system safety engineering courses are presented, each two weeks in length.

IV. The course, Quantitative Methods of Safety Analysis, is a recent addition to the graduate courses presented by the Institute Safety Division. The basic premise of this course is that system safety analysis should be a process which is fully capable of assuming a leading role in design analysis. The basic purpose of system safety analysis should be, therefore to identify hazards in the system as it is proposed to be designed and operated, evaluate the risk associated with the identified hazards, and eventually to prevent or control the hazards which are considered to be unacceptable. This course provides technical knowledge in the system safety analytical technology and associated quantitative risk assessment methods. Most importantly, effective utilization of the output of the safety analytical program is emphasized in the instructional material. The student is introduced to the philosophy of risk acceptance, the derivation and allocation of risk requirements, and the quantitative risk evaluation methods.

SYSTEM SAFETY IN OPERATIONS

The conventional application of the system safety engineering process to the earlier design phases of the system life cycle has sometimes led to a lack of awareness of the technical safety aspects during operations. Utilization of the modern system safety analytical technology is being restricted almost entirely to the design phases as previously noted. Furthermore, system safety educational programs normally do not include System Safety as a formal, disciplined approach in the operational phase. Recent developments have been made at U.S.C. which should improve safety decision-making during the operational phase. These developments represent new and improved analytical methods for use during operations which were derived from the system safety technology. Accident Logic Diagramming is a good example of the adaptation of a system safety analytical method to assist the accident investigator in identifying accident cause factors. The field of accident investigation has developed into a highly specialized body of technical knowledge. There are files which are literally full of accident cause data, hoping that through knowledge of the cause of accidents we can take action to prevent future accidents. It is possible that rather than logically identifying real causes of accidents, the accident investigator is doing nothing more than confirming his preconceived conclusions. In order to minimize this possibility, the investigator should utilize a logical, systematic, and thorough approach which is more analytical in nature in order to isolate and identify accident causes. A method of system safety analysis which has been developed over the past ten years termed Logic Diagram Analysis or Fault Tree Analysis, is ideally suited to this task. The logical processes of fault tree development are in fact identical to the logical processes of accident investigation. The investigator and the analyst deduce from available evidence, beginning with the fact of the accident or pre-accident itself until the probable cause can be identified and substantiated. Utilization of this analytical tool by the investigator to organize his thinking is termed Accident Logic Diagramming. Standard event and logic gate symbology have been developed and may be consistently applied to actual accident situations. However, for the purposes of accident investigation, certain modifications to the basic logic diagramming system are required. Since the undesired event in question has already occurred, then the matter of event probabilities and quantitative risk evaluation is not necessary. Accident Logic Diagramming is strictly a qualitative assessment. As a result all possible causative conditions can be logically diagrammed, regardless of the availability of numerical failure data. The man, the machine, and the environment can be logically combined as an interacting system.

Several obvious advantages are realized with Accident Logic Diagramming. First, the logical thought processes are presented in a visible, logical, easily understood diagram for others to see and comment upon. This factor alone increases the likelihood that ideas will be shared and investigative methods will be questioned. Second, a documented, graphical checklist of areas to investigate logically develops with the diagram, minimizing the possibility that important evidence will be overlooked early in the accident investigation. Finally, the Accident Logic Diagram becomes a flow chart and a realistic indicator of investigative progress. Notes on evidence can be made next to the diagram events to which they apply, indicating whether the events did or did not occur. It is recommended that the Accident Logic Diagram be prepared as early as possible in the investigation cycle, and that it be continually expanded. Eventually as the actual accident cause factor(s) is isolated and identified, necessary corrective actions can be taken, thus reducing or eliminating the possibility of future accidents due to similar cause factors.

CONCLUSION

General John D. Ryan stated, "The application of measures to achieve higher levels of System Safety is recognized today as a vital concern for the entire engineering community as well as for our managers and operators. This goal is clearly essential, because it represents the principal means of preserving the combat capability of the Air Force. We, therefore, must consciously focus our efforts on reaching that goal. . ." System Safety is a

vital concern in the achievement of accident prevention. The application of the System Safety concept in design and in operations should be a principal means of avoiding all conceivable situations which can place our nation, its resources, or its population in jeopardy. As our nation continues to design and manufacture equipment which is more expensive, more complex, with greater degrees of automation for use by and around a public which is aroused and more intelligent, System Safety becomes increasingly important. As a result, System Safety education is also becoming increasingly important. At the University of Southern California, as safety educators we are confident and optimistic that the challenges of System Safety education will be met.

N72-25971

SYSTEM SAFETY EDUCATION FOCUSED ON INDUSTRIAL ENGINEERING

W. L. Johnston and R. S. Morris
Texas A&M University

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

No field of engineering enjoys closer relationship to public and political concern today than safety engineering; and probably no other engineering field is so ill prepared to exploit this relationship. Why! Because the demands on the safety engineer today require thorough understanding of systems analysis and systems engineering principles, human factors, and the safety implications of hardware design. Unfortunately, most safety engineers developed from other specialities and are primarily experienced in industrial safety. The rapidly expanding technology of today's world requires solution of potential safety hazards by recognizing the hazards and appropriately influencing the design of hardware to eliminate or reduce them.

Nowhere has the short supply of safety engineers, with the necessary background, been more sharply felt than in the Army Materiel Command. The primary mission of this command is the research and development, procurement, and supply of Army military hardware. The bulk of the system safety responsibility for this hardware rests with the Army Materiel Command Safety Office and similar offices at the subcommands (called commodity commands because of their commodity orientation). This safety organization has, until recently, been primarily concerned with industrial safety at production activities within the Army Materiel Command (AMC). There is increasing recognition by both the general public and development personnel that most accidents resulting in property damage, injury, and loss of life are casued by and/or compounded by hardware not designed for the human environment. The natural outcome of the recognition has been to place greater responsibility for hardware design on the AMC safety organization.

Having been staffed primarily by non-engineering safety personnel during World War II, AMC faced a critical shortage of the necessary skills. A large portion of its existing safety staff will be retiring in the next five years. AMC and especially Mr. Landon Feazell, the present Chief of the AMC Safety Office, recognized the impending safety personnel shortage and made provisions to improve the outlook.

Basically, the AMC requires the input of 20 to 30 engineers per year with thorough knowledge of system safety and its related principles - personnel who can both influence design and revitalize the safety workforce, moving it into its proper realm of responsibility. To accomplish this would require hiring younger engineers with good safety engineering background or training. Unfortunately, this kind of engineer is difficult to find and even more difficult to hire. The best alternative was for AMC to train their own personnel and a training program was established to accomplish the following objectives.

1. Recruit into the AMC workforce young, qualified engineers with demonstrated capability.

2. Educate these engineers in the field of safety engineering. Also, educate them in the specifics of Army peculiar safety hazards incumbent with the development and handling of explosives, nuclear weapons, and the chemical/biological agents.

Since a good background in hardware design is essential to the functions of system safety, engineers with specialization in Mechanical, Electrical, Civil, Aeronautical, or Chemical engineering are desired. To obtain the very best engineering graduates AMC in conjunction with Texas A&M University, established a graduate level training program giving the student the opportunity to obtain a Master of Engineering Degree. To provide the necessary theoretical background, as well as the practical background, in hazardous materials requires two years of classroom study. The engineers upon graduation are placed in safety positions at all AMC activities. Since they are trained by the AMC Intern Training Center, the graduates have broad knowledge of AMC safety functions with no built in loyalties to specific commodity areas. They provide AMC with a highly capable, flexible, and mobile safety engineering expertise. A description of the curricula for the Safety Engineering Program follows.

CURRICULA

This jointly sponsored Safety Engineering Program consists of twenty-four months of graduate level study divided into three sections: (1) the first six months of the program are taught by the USAMC Intern Training Center at the Red River Army Depot, Texarkana,

Texas; (2) the next 12 months are taught by Texas A&M University - with the first eight months taught at the Red River Army Depot Extension, while the last four months are taught on the main campus at College Station, Texas; and (3) the final six months are taught by the US Army Field Safety Agency at Charlestown, Indiana.

During the first two phases (first 18 months) all of the courses are graduate level and are presented in a university environment. A breakdown of the program of instruction by major topic area is shown below:

SYSTEM SAFETY RELATED COURSES (21 Credit Hours)

*Introduction to Safety Engineering
System Safety Engineering
System Safety Engineering in the Design of Equipment
Safety Engineering in Facilities Design
Safety Engineering in Transportation Systems
System Safety Seminar
Safety Engineering Research

*Non Graduate Credit

These courses are designed to provide the students with specific background material which will allow him to serve as a system safety specialist on a design team. Discussion concentrates on the application, selection, and utilization of various system safety analytical approaches. Emphasis is also placed on the management of a system safety program, its relationship with other disciplines, and new developments and applications of system safety techniques.

SYSTEM SAFETY INTERFACE COURSES (22 Credit Hours)

*Statistical Methods in Reliability and Maintainability
*Weapon System Acquisition
*Engineering Application of Computers
Theory of Human Factors Engineering
Engineering of the Man-Machine Systems
Evaluation and Control of the Occupational Environment

*Non Graduate Credit

This set of courses is designed to provide the graduates with a working knowledge of Human Factors Engineering, Maintainability Engineering, Reliability, Industrial Hygiene, and the System Acquisition Process. All of these as you well know are very closely related and are important inputs when the total safety of the system is under consideration.

INDUSTRIAL ENGINEERING COURSES (30 Credit Hours)

*Introduction to Operations Research
*Mathematical Statistics
*Applied Mathematics
*Engineering Management
*Statistical Quality Control
Analysis and Prediction
Principles of Operations Analysis
Advanced Quality Control

*Non Graduate Credit

These courses serve three purposes. First of all they serve as pre-requisite type courses in order to bring all the different type engineering graduates to a common plane for the more advanced courses which follow. Secondly, the courses strengthen the student's mathematical abilities which are important in applying system safety and reliability analysis. Finally, since a Master's Degree is offered through the Industrial Engineering Department, certain "core" course are required by the Graduate College of Texas A&M University in order to award this degree.

The last phase of the program is conducted at the US Army Field Safety Agency and is designed to provide practical "hands on" type of training. The formal training includes both Army and AMC procedures, safety regulations, and related exercises in practical applications of safety principles. A portion of the program is devoted to "on-the-job" type training.

The major topics that are covered in this phase are:

FIELD SAFETY AGENCY TOPICS

On-Job Orientation
Munitions Safety
Aviation Safety
Industrial Safety

System Safety
Radiological Safety
Safety Management

As you can readily see from the curricula ove, these engineers are being trained for uch more than just "system safety engi- ieering" as we have come to think of it during ecent years. By taking the total engineering pproach to system safety education, these raduates will have more capability in a much broader area of responsibility. A majority of he AMC installations at which these graduates will be assigned have no formal "system safety" organization. At many of these commands it will be a part of their duties to help initiate system safety activities. At still others he individuals may have to input system safety through such organizations as Research & Development, Quality Assurance, etc. After gaining invaluable experience on the job we feel these graduates will be capable of integrating into any system development team, and will be able to improve design through appli- ation of system safety engineering principles.

ENTRANCE REQUIREMENTS

The requirements for the engineering graduate input to this program are the same as the requirements for the other two intern programs (Production Design Engineering and Maintainability Engineering) which the USAMC Intern Training Center administers. Graduate engineers are recruited from universities across the nation, representing different engineering disciplines, from the upper one-third of their graduating class. With this academic ranking the students enter Federal Service as GS-7 Quality Students. After satisfactorily completing the first 12 months of the program they are promoted to GS-9 grades, and after successful completion of the 24-month program they are promoted to the grade of GS-11. At the end of the 24-month program each graduate assumes a three year continued service agreement with monetary repayment if they leave the Federal Government prior to the expiration of the three years.

FIRST CLASS

The first class of safety engineers began their study in June 1969. Their average undergraduate grade-point was 3.1 on a 4.0 system and they represented 15 different universities from across the United States. All 20 students received Master's Degree from Texas A&M University in August 1970 and have just this month completed the 24-month program and have been given permanent duty assignments at various AMC installations.

The second class has just completed the first 12 months of the program and the third class has been recruited and will report June 1 to begin training.

CONCLUSION

Since one of the objectives of this conference is "applications" and "transfer of information" it should be pointed out that while the program described in this paper is a specific program for AMC, a similar program is available on an individual basis at Texas A&M. Here the individual would choose his own degree program and would usually require 12 months to attain a Master's Degree in Industrial Engineering, assuming he has a Bachelor's Degree in any field of engineering. Individual students are encouraged to adapt the techniques and philosophy of "system safety" to "product safety" as it is commonly referred to by private and consumer industry. Indeed, it has been said that one of the more important spin-offs from the aerospace technology may be the system safety concept and its application to product safety.

The USAMC-Texas A&M program in Safety Engineering is an effective method for educating and training engineers in the unique and demanding technology of system safety engineering. As these graduates progress through AMC assuming positions of responsibility, they will make their presence felt and will have a tremendous impact on not only AMC, but the US Army as well, the principal customer of AMC commodities. Improved safety performance, monetary reward from reduced costs, and upgrading the overall capabilities of the AMC safety workforce are the expected results from this program.

The first class of the "System Safety" course at The George Washington University was held in March 1969. This two-week, non-credit course was offered twice in 1969, three times in 1970, and it is scheduled at least four times in 1971. So the course is in an expanding mode.

The course was initiated with the support and guidance of the Electronics Industries Association G-48 "System Safety Committee," chaired by George Mumma of the Martin Marietta Corporation. Mr. Mumma also serves as a guest lecturer in the course. Numerous notables in the field of system safety contribute as guest lecturers in the course including the Chairman of this Conference, Phil Bolger, and Jerry Lederer, NASA Director of Safety. In addition to Messrs. Bolger and Lederer, the following men listed in the program for this Conference have served as lecturers in this course: C. O. (Chuck) Miller, Dr. Carl C. Clark, Haggai (Guy) Cohen, and Dr. Raymond M. Wilmotte.

COURSE RATIONALE

Course Scope

At GWU, system safety covers the total spectrum of risk management. While starting with the dynamic system element (vehicle, machine, or process), the course examines the influence on system safety of attitudes and motivations of design, production, test and operations personnel, employee/management rapport, the relation of industrial and labor associations among themselves and with the Government, human factors in supervision, the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical operating personnel, political considerations, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control.

Not only does the course cover a wide range of subject matter. It is designed to introduce the principles, requirements, techniques, and limitations of system safety to those charged with hazard or risk control in the following fields: urban planning, environmental control, mass transit, automotive safety, hospital administration, accident investigation, insurance underwriting and campus safety.

Three Titles - The GWU course is not as directly related to the military services as other system safety courses offered throughout the country. Both the University of Southern California course and the one presented by the University of Washington are sponsored by the United States Air Force. The course taught at Texas A&M University is under the direction of the United States Army Material Command. Nonetheless, students from all the military services have been and continue to be enrolled in the GWU course.

Carrying out the theme of this Conference--"to expand the application of system safety principles into the general and consumer industries"--GWU advertises its course under three titles. The purpose of multiple titles is not to confuse anyone but rather, to hopefully match impedances with other industries beside aerospace.

Obviously, the course is advertised as a "System Safety" course because this term is commonly understood in the aerospace industry, the military establishment, and in NASA.

Attempting to communicate with a completely foreign segment of the economy, GWU offers the course as one in "Hazard Control." Those who would understand this term much easier than they would the term, "system safety," include insurance underwriters, hospital administrators, or perhaps those associated with the mining industry.

Still another portion of industry is introduced to the course under the title, "Risk Management." This group could include urban planners, campus safety managers, and even professional football team owners!

ASSE Sponsorship - The breadth of scope, titles and application described above was a prime factor in the decision of the American Society of Safety Engineers, representing approximately 10,000 safety professionals, in January 1971 to co-sponsor the GWU course. This action by ASSE was unique as it marked the first and only official endorsement of any university educational activity by that organization.

N72-25972

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT

Mr. Vernon L. Grose
George Washington University

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

Student Contribution

The GWU course is purposely designed to utilize and integrate the diversity of experience represented by the students attending the course. This position is in contrast to courses where the instructors supposedly have all knowledge on the subject "wrapped up in a box with a blue ribbon around it." Rather than "pipe knowledge in a straw to naive students," the instructors view classroom discussion as a learning experience every bit as valid as formal lecturing

The diversity of backgrounds possessed by graduates of previous classes makes this point obvious. Students from at least seven categories have completed the course:

Commercial Industries - American Mutual Liability Insurance Company, Ebasco Services, Incorporated (major contractor), De Leuw, Cather & Company (engineering contractor for the Washington Mass Transit), and Western Electric.

Aerospace Industries - General Dynamics, Ling-Temco-Vought, Martin Marietta, McDonnell Douglas, and Vitro Laboratories.

Federal Government - Federal Highway Administration, Atomic Energy Commission, Bureau of Mines, Federal Aviation Agency, National Transportation Safety Board, National Bureau of Standards, and National Aeronautics and Space Administration.

Foreign Governments - Department of Social Action (Mexico) and British Aircraft Corporation.

City/County Governments - Chicago Transit Authority, New York City Transit System, and Montgomery County (Maryland).

Military Services - Numerous branches within the Army, Navy and Air Force

Universities - Johns Hopkins University and The George Washington University.

APPROACH TO SYSTEM SAFETY

The GWU course starts off by defining the problem. As Figure 1 states, "We are trying to do well that which we do not understand." Furthermore, we will never understand that which we must do well. Dr. Raymond M. Wilmotte reaffirms this statement in different language:[1] "The uncertainties that remain (in any complex decision) are never zero."

The reason for this pessimistic outlook is quite simple. The complexity of most situations faced by decision-makers today is far beyond any single individual's capability to comprehend them in depth. Yet we are precluded the luxury of simply wringing our hands in despair--we must still press forward and make decisions.

"Systems" Characteristics

The systems approach, regardless of its application, has at least eight characteristics as shown in Figure 2. Since system safety can be described as "the systems approach applied to safety," these eight traits apply directly to system safety. Further, these characteristics differentiate system safety from other safety activities.

A description of each characteristic is repeated from an earlier publication:[2]

Methodical - The systems approach involves a definite method. This method consists of an orderly procedure or way of solving complex problems. All the steps involved in problem-solving are arranged in a consistent and orderly manner.

Objective - The systems approach is also objective; i.e., the steps in the problem-solving method are free from personal bias to the greatest extent possible. Personal opinion must be identified as such. By maintaining this discipline, the results of each step in the problem-solving process can be verified or confirmed by someone other than the person who performed the step.

Quantitative or Measurable - Almost without exception, each element in the problem-solving process results in a quantitative expression. At the very least, there must be some measurement possible to weigh the validity of the conclusion reached. Because any end product produced by the systems approach is obviously a compromise, it is necessary to weigh the relative merits of each element in the system by some means other than personal opinion. This need to compare alternatives dictates that measurability be

one of the characteristics of the systems approach.

Analytical - The systems approach employs a rational division of the whole system into its constituent parts to find out the nature, proportion, function, and interrelationship of these parts as they contribute to system objectives. This analytical function frequently leads to solving system problems by means of mathematical models or equations. Thereby, the elemental variables can be related and traded off with respect to each other.

Subsystem Interdependence - Another characteristic of the systems approach is a constant recognition that any given element or subsystem is dependent on all the other elements in the system. Should the function, dimension, or description of a subsystem be revised, such a revision will affect every other element to varying degrees. This interdependence must not only be acknowledged but must be accounted for in the systems approach.

Parallel Analysis of Elements - Somewhat related to the interdependence of all elements and subsystems in the systems approach is the concept of treating all elements in parallel rather than in series. In contradistinction to the Western civilization concept of time as being a chronological series of events, each one of which must be complete before the next can take place, the systems approach demands that the end event be considered at the same time as the initiating event in order to properly balance the allocation of resources toward solution of the problem. This is commonly known as "womb-to-tomb" thinking.

Inputs and Outputs in Clear Language - Another important characteristic of the systems approach is the requirement that both inputs and outputs, at all levels in the system, be described in unambiquous language. The key to this requirement is that it removes subjective judgment both as to what is expected in the way of outputs and what is available in terms of inputs to the system. One of the reasons for insisting on the quantitative indices discussed earlier is that numbers do reduce ambiguity.

In simplest terms, a "system" can be defined as "any complete entity consisting of hardware, software, personnel, data, services and facilities which transforms known inputs into desired outputs." Therefore, a system has no meaning unless both inputs and outputs have clear and universal understanding.

Self-Containment/Closed Loop - Since a system has been defined as a "complete entity," this means that a system has individual existence and that it lacks none of its requisite parts. It is complete in itself. A corollary is that the system must be free from any isolated or "orphan" elements which do not contribute to system objectives. Outputs of every element or subsystem must ultimately become part of the system output rather than independent of it. In a sense, this is a restatement of the fact that everything within the system is interdependent.

The Role of the Human

One difficult that must be acknowledged in the field of safety is the high pe ·entage of social behavior involved in hazard analysis and prevention. Therefore, the emphasis on human behavior is quite pronounced in the GWU System Safety course. Whether it be called human factors, human engineering, or just plain human awareness, the role of the human is accented heavily.

Figure 3 illustrates the interface that exists between physical and social sciences. Skirting the traditional battle over whether social sciences are "scientific," predictability (which is a cornerstone of scientific endeavor) is an elusive characteristic, at best, in the social sciences. To illustrate this difference between physical and social sciences, the specific gravity of sulfuric acid (H_2SO_4) has been, is, and will continue to be 1.834, whereas you and I had not been, are not, and never again will be the same persons we were when we awoke this morning!

There will always be a mixture of physical and social forces in any system. However, the mixture ratio will influence the applicability of the systems approach. The higher the percentage of systems effort which involves the physical sciences, the greater the applicability.

The spectrum of system problems in Figure 3 runs from greatest applicability on the left end to least on the right. System safety, as an activity, would probably fall about where "auto safety" is shown. We can do much to make

cars safer--crash helmets, harnesses, inflatable bags for crashworthiness. But in the end, can the automobile be made totally safe if the human is ignored? Obviously not. We can never make people wear seatbelts, helmets or chest protectors. Further, we cannot stop them from driving after they have been drinking! My good friend and colleague, Chuck Miller, has said that we probably should start to design cars to be driven by drunk drivers because there is no way to stop people from driving while drunk.

This pragmatic outlook of accepting the world as it is, rather than idealistically teaching "what ought to be" distinguishes the GWU course from some others.

System Management Foundation

System safety may be the foremost among those activities where moral arguments must be translated or converted into specific tasks. Furthermore, this "conversion into tasks" must ultimately result in specific safety tasks which are described in the language of management--yes, that dirty but real world of cost, performance and schedule!

In a letter dated 14 January 1971, General George S. Brown, Commander of the Air Force Systems Command, said in part:

> "Reports of the USAF Inspector General continue to reflect that systems safety within AFSC is unsatisfactory. There are several underlying problems in this area, including the need to train systems safety engineers. To overcome these problems we must have added management emphasis on systems safety at all levels." (Italics added)

The System Safety course at the George Washington University is based firmly on a SYSTEM MANAGEMENT foundation for a number of compelling reasons:

1. Management and professional system safety personnel both have one basic modus operandi-- "accomplishing through others." While they both may occasionally get in, roll up their sleeves, and "do" something, this is a rare exception. Learning how to step back from the daily rush of detail activity to view the "big picture" of the systems approach is vital to effective system safety work. Further, if the system safety professional accepts a role as simply an "engineer," "analyst," or "investigator," he cannot hope to accomplish his mission because these "doing" roles are only partials of a whole picture.

2. A corollary to the first reason is that since system safety personnel "assure that a system is safe" rather than personally "make the system safe," they must have a 1:1 communication link with management. How can they hope to communicate with top management if they take less than a system management viewpoint? How will they know the system management viewpoint if they have not studied it?

3. One of the major advances of MIL-STD-882 over earlier system safety specifications was in pioneering the concept that system safety was far larger in scope than just "engineering." To state this idea another way, you could be the best safety engineer, analyst or investigator in all the world and still be no more effective in achieving system safety than if you were in Tibet, if you fail to comprehend system management.

4. A primary precept of system safety is that no area or activity in the system development process is free from creating hazards. Therefore, since system safety personnel must be sensitive to all sources of hazards (and management is a hazard source as shown in the Venn diagram of Figure 4), it is imperative to start the study of system safety on the base of system management, the most pervasive activity in system development.

It is no accident that management is listed prior to science and engineering in this definition used in the GWU course:

> "System safety is the optimum degree of hazard elimination and/or control within the constraints or operational effectiveness, time and cost, attained through the specific application of management, scientific and engineering principles throughout all phases of a system life cycle."

The interrelationship of man, machine, media, and management in Figure 4 contains 15 different categories; e.g., man/media, machine/management, media/man/machine/management, etc. Each one of those categories is a source for system hazards which must be either eliminated or controlled.

Using rapid rail transit as an example in Figure 5, management is prominent as a factor in contributing to hazards. As a warning, it should be obvious that Figure 5 ignores the interaction between the factors listed; e.g., possible interaction between passenger vehicle seat versus stand ratio and accident investigation procedures.

Likewise, most of the individual events shown in the Fault Tree illustration in Figure 6 have resulted from management decisions; e.g., policies, procedures, design selections or accepted risks. Note also the high percentage of events in the Tree that are social rather than physical in content.

Figures 4, 5, and 6 are not meant to be exhaustive and complete but to simply trigger further thought and expand the analyst's thinking regarding hazard sources. In fact, the GWU course is often described as a "mind expander." An attempt is made to open up new ways of thinking about hazards, followed by devising methods to either eliminate or control the identified hazards.

Integrative Aspect

A prime thesis of the GWU course is that system safety is not another "specialty" but an integrative activity among the already-too-many specialties. Figure 7 depicts system safety as the "mortar between the bricks" that makes possible a strong wall (system). In other words, the philosophy of the course is that system safety personnel should not be "out-designing the designer." Rather, they should be concentrating their attention on the many interfaces created between functions whenever a large and complex system is divided up into smaller units.

As Figure 7 shows, "design" is separated from "testing," and when this division occurs (necessary as it may be), there are inevitable problems often overlooked by both designers and test engineers. This interface is typical of those areas where system safety personnel will realize the greatest payoff in terms of hazard potential.

FOCUSING FOR MANAGEMENT DECISION

The system safety professional has only one ultimate "reason for being"-- to provide top management with one of two inputs for management decision: (1) the system under consideration is safe enough, or (2) the system under consideration still has the following identified hazards which are neither eliminated nor controlled satisfactorily to meet the system objectives.

As stated earlier, safety is basically a moral argument; i.e., "No one should get killed or injured and there should be no property loss as a result of operating this system." Unfortunately, there are literally millions of moral arguments of equal conviction. Management has no way to handle moral arguments. They do not fit nicely into equations, calculations, or profit/loss ledgers. They must be converted into a new language.

How can safety then be translated into management language? What is the language of management? Management language is three-dimensional-- cost, performance and schedule. To bridge the gap then between a moral argument and the world of cost, performance and schedule, there must be a methodology.

In a nutshell, the methodology required has five basic steps:

1. All possible hazards must be identified.
2. These identified hazards must be ranked first for their severity.
3. These identified hazards must be ranked secondly for their likelihood of occurrence.
4. These identified hazards must be ranked thirdly for the cost, in resources, of either eliminating or controlling them in the system.
5. The rankings of steps 2, 3, and 4 must be combined into a single ranking of management consequence; i.e., where the most severe which will occur most frequently and can be eliminated for the least resource expenditure are on top.

Each of the five basic steps required to translate the moral argument for safety into language that any manager can understand is discussed briefly.

Step 1 - Identify Hazards

This is the function of the various analytical techniques such as Hazard Mode and Effect Analysis (HMEA), Gross Hazard Analysis, and Fault Tree Analysis. Equally essential with

these techniques are analysts with inquisitive, imaginative, and indefatigable minds. Ironically, some system safety courses cover only this first analytical step.

Step 2 - Rank Hazards for Severity

Continuing to use rapid rail transit as an example, Figure 8 is a conversion of the four hazard levels of MIL-STD-882 into rail transit effects. Rather than having everyone decide what a "critical" hazard is, the translation has been made so that there is universal understanding of this level. If there were 478 hazards identified in Step 1, then every one of the 478 should have either an A, B, C, or D assigned to it.

Step 3 - Rank Hazards for Likelihood

After all 478 identified hazards have been categorized for severity, they must be ranked for probability of occurrence. One example of how this might be accomplished is shown in Figure 9. The reason that the four levels of probability are in a logarithmic scale is because the human response to sensory stimuli, according to Fechner's Law, is logarithmic. Perception of probabilities is probably similar to sensory perception. When this step is complete, all 478 identified hazards should have two letters assigned-- one for severity and one for probability.

Step 4 - Rank Hazards for Elimination/Control Resources

The third letter to be assigned each of the 478 hazards should be from a table such as shown in Figure 10. This step requires an intermediate conversion of various resources (e.g., policy, procedures, manpower, technology, facilities, materials, and schedule) into a dollar equivalence prior to selecting a code letter. Nevertheless, this estimate of the amount of resources is essential in order to speak management's language. Now all 478 hazards have three letters assigned.

Step 5 - Rank Hazards for Management Consequence

Once three code letters (one each from Steps 2, 3, and 4) have been assigned to all 478 identified hazards, the focusing for management consequence is achieved by combining the three individual code letters into one overall index of significance. The Hazard Totem Pole shown in Figure 11 lists these code combinations in order of consequence for management decision.

Obviously, there are never enough resources to completely eliminate every possible hazard. For this reason, management must set a "decision point" or cutoff level in the Hazard Totem Pole. This decision point is drawn at that significance ranking code below which all remaining hazards will be ignored. The decision point may be established by either (1) the reduction of hazard significance to a level which management considers adequate or (2) the depletion of resources available for application to hazard elimination or control.

To illustrate this decision point, management could decide that it will eliminate and/or control all hazards in the first 7 levels or categories in the Hazard Totem Pole; i.e., all the AJP, AJQ, AKP, BJP, AJR, AKQ, and ALP hazards. This would mean that 31 of the 478 identified hazards will require resources to be allocated by management for purposes of eliminating or controlling the hazards. (Note that there were no AJQ or AKQ hazards.)

It is important to also note that while management will be committing resources for the first 7 levels in the Hazard Totem Pole, they will, by this very action, be deliberately ignoring all remaining 57 levels in the Hazard Totem Pole (which contain the remaining 447 hazards!). Therefore, the decision point becomes that point which separates action from inaction regarding hazards.

RESOLUTION OF HAZARDS

MIL-STD-882 describes a series of actions for satisfying safety requirements of a system design. The series is known as "system safety precedence." This precedence is shown in logic diagram format in Figure 12.

Continuing the rapid rail transit example where management has now decided to eliminate or control 31 of the 478 identified hazards in the Hazard Totem Pole, a decision must be made on HOW to eliminate or control them. Figure 12 shows four alternatives (numbered 1 through 4) for this decision.

With the exception of those hazards which can be eliminated very economically early in the design stage, the four alternatives of Figure 12 are numbered in a hierarchy of decreasing effectiveness as well as decreasing cost. Therefore, the lower the number in the hierarchy, the more effective the choice will be in satisfying system safety requirements even though there may be higher cost associated with the action. (A more detailed discussion of this concept appears in Reference 3.)

The dotted lines in Figure 12 illustrate something not discussed in MIL-STD-882. Two conditions, both of which are undesirable, are shown in dotted lines. First, a system can be tolerant to identified hazards without the knowledge of either designers or operators. Secondly, the system can be intolerant to identified hazards, either unknowingly (most serious) or knowingly. Hazards which are knowingly intolerable are often described as "accepted risks." Those risks are the ones for which insurance is purchased.

REFERENCES

1. Wilmotte, Raymond M., "Communication of Risk," "Proceedings of the Second Government/Industry System Safety Conference, Goddard Space Flight Center, 26-28 May 1971.

2. Grose, Vernon L., "Constraints on Application of Systems Methodology to Socio-Economic Needs" Proceedings of the First Western Space Congress, 27-29 October 1970, Santa Maria, California.

3. Grose, Vernon L., "System Safety in Rapid Rail Transit," as presented to the Rail Transit Conference, sponsored by the American Transit Association and the Institute for Rapid Transit, San Francisco, California, 13-16 April 1971.

THE PROBLEM

Trying to do well that which we do not understand

Figure 1

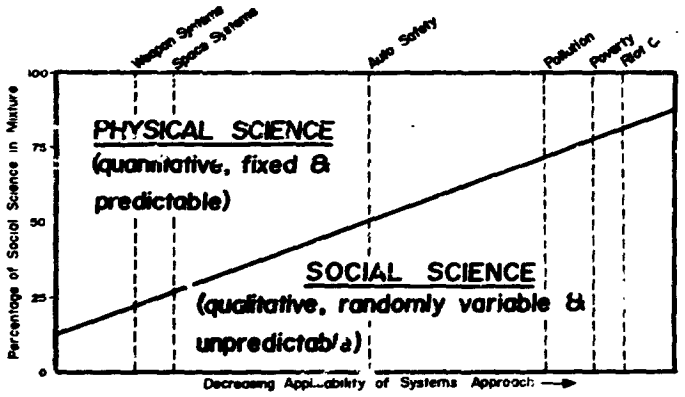
SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose

- Methodical
- Objective
- Quantitative or Measurable
- Analytical
- Subsystem Interdependence
- Parallel Analysis of Elements
- Inputs & Outputs in Clear Language
- Self-Containment/Closed Loop

"SYSTEMS" CHARACTERISTICS

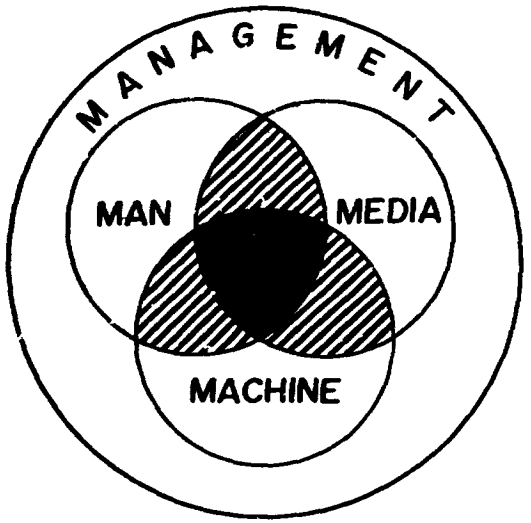
Figure 2

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose



The Science "Mixture Ratio" in the Systems Approach

Figure 3



Interrelationship of System Safety Factors

Figure 4

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose

SYSTEM SAFETY

"The Strength Between Functions"

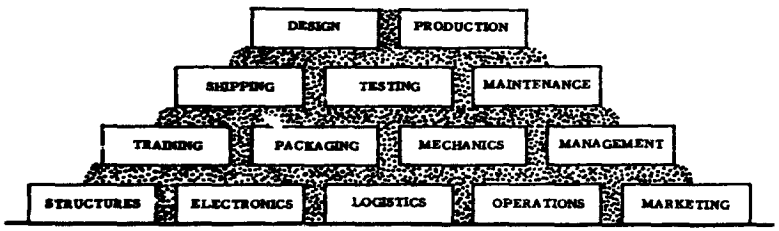
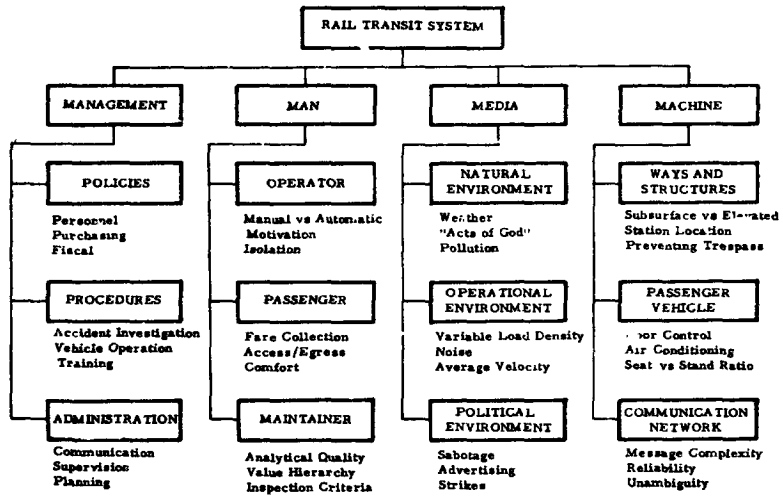


Figure 7

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose



TYPICAL SYSTEM SAFETY FACTORS IN RAPID RAIL TRANSIT

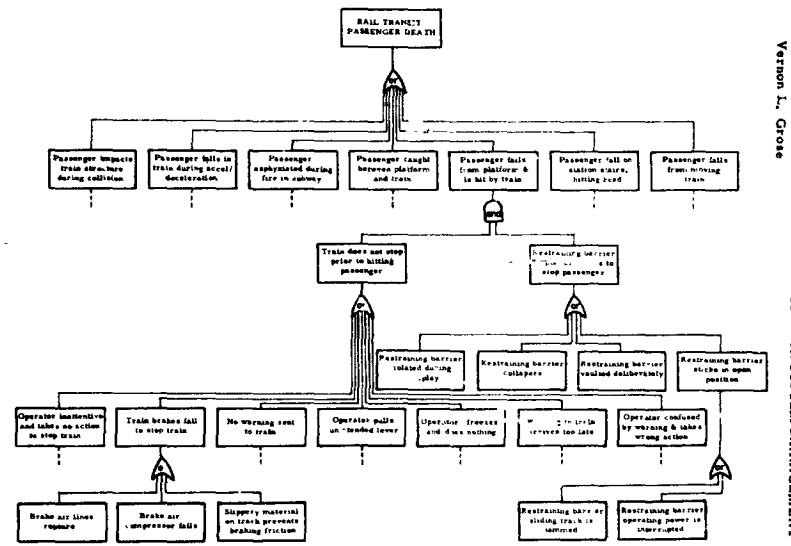
Figure 5

CODE	MIL-STD-882 HAZARD LEVEL	EFFECT ON SYSTEM OBJECTIVES	EFFECT ON FUNCTIONAL CAPABILITY	EFFECT ON PERSONNEL SAFETY
A	Catastrophic	Rail transit rendered impossible-- Mission is lost	No portion of rail transit system can be salvaged-- Total loss	Personnel suffer death or multiple injuries by factors in Code B
B	Critical	Rail transit impaired seriously-- Mission accomplished only by auxiliary methods	Two or more major sub-systems of rail transit are damaged-- This condition requires remote depot maintenance	Personnel injured either: (1) operating the transit system, (2) maintaining the system, (3) being transported by system, or (4) being in vicinity of the transit system
C	Marginal	Rail transit is possible by utilizing available redundant operational options	No more than one component or subsystem damaged. This condition is either repairable or replaceable within one hour on site	Personnel-injuring factors in Code B can be controlled by either automatic devices, warning devices or special operating procedures
D	Negligible	No measureable effect on rail transit mission	No apparent damage to the rail transit system	No injury to personnel

HAZARD SEVERITY FOR RAIL TRANSIT SYSTEM

Figure 8

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose



Rail Transit Fault Tree Illustration

Figure 6

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose

CODE	DESCRIPTION OF SITUATION
J	Hazard of interest will occur within 10 cumulative hours of operation
K	Hazard of interest will occur within 100 cumulative hours (4 cumulative days) of operation
L	Hazard of interest will occur within 1000 cumulative hours (41 cumulative days) of operation
M	Hazard of interest will occur within 10,000 cumulative hours (14 cumulative months) of operation

HAZARD PROBABILITY FOR RAIL TRANSIT SYSTEM

Figure 9

CODE	CALCULATED DOLLAR EQUIVALENCE*
P	Less than $1000 required to eliminate/control this hazard
Q	$1000 - 10,000 required to eliminate/control this hazard
R	$10,000 - 100,000 required to eliminate/control this hazard
S	Over $100,000 required to eliminate/control this hazard

*Calculated dollar value of all resources (revision of policy, procedures, manpower, dollars, technology, facilities, materials, and schedule) required to either eliminate or control the hazard of interest.

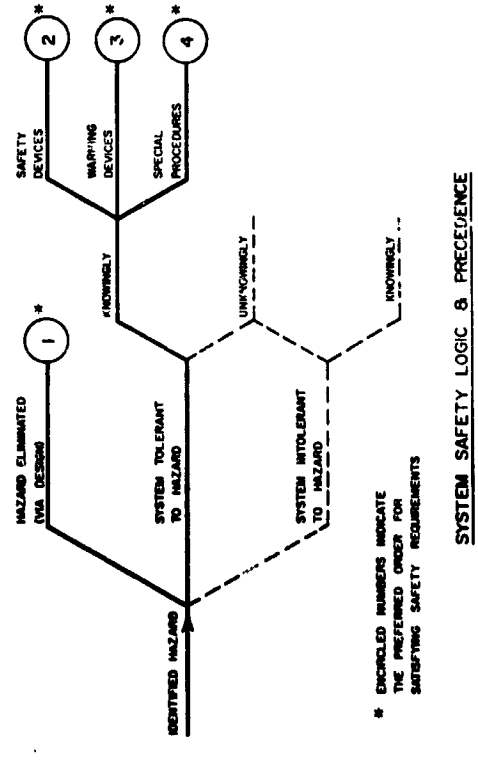
HAZARD ELIMINATION/CONTROL RESOURCES

Figure 10

Hazard Significance Ranking	Code Combination			Number of Rail Transit System Hazards
	Hazard Severity	Hazard Probability	Hazard Resources	
1	A	J	P	3
2	A	J	Q	None
3	A	K	P	1
4	B	J	P	16
5	A	J	R	7
6	A	K	Q	None
7	A	L	P	4
8	B	J	Q	22
64	D	M	S	2

HAZARD TOTEM POLE

Figure 11



SYSTEM SAFETY LOGIC & PRECEDENCE

Figure 12

SECTION III

QUESTIONS AND ANSWERS

QUESTION: I would like to ask the panel if there is any concerted effort in the educational field to incorporate a system safety engineering course in all undergraduate engineering programs -- aeronautical, industrial, electrical, etc.

DR. JOHNSTON: We can only speak for the industrial engineering department. As far as I know Texas A&M has none. Actually what we are looking at in a system safety engineering course as far as for a person working on a degree in mechanical engineering or something at the undergraduate level, this would have to be an elective. What we are doing at Texas A&M is trying to make people in all the engineering disciplines aware, probably more so toward product safety and product liability. We are getting more and more people to come in and take the courses as electives, but as far as a requirement, I would say there is no attempt to put it into the undergraduate discipline across the board. Most all of the people that take or get a B.S. in industrial engineering will take a course in system safety engineering as it is offered.

MR. GROSE: Gene I don't know if you care to respond to this or not, are you aware of any activities at USC where they have tried to introduce this?

EUGENE HOLT: I don't think that is necessarily a good idea. Outside of a system safety curriculum or a safety program, the only way to incorporate system safety engineering into EE or ME courses, I think would be in each basic course and that would be rather hard to do. I think because of the basic structure of universities and the way curriculums are established, etc. it would be hard to do that. It is a good idea but at present it is not workable I am afraid.

JACK MANSFIELD (GWU): It is about the same answer you just got from Gene Holt. This was discussed very recently at a system safety society meeting here in Washington. As a matter of how to get this into an undergraduate, should something be put in. I think it will not come by the university taking the initiative on it. If it comes it is going to be by societies or conferences or things making recommendations and putting a little pressure on universities to get something like this as a part of some undergraduate course. I don't think a complete course itself would be of value because it would be an elective almost certainly and would not cover a great many people. A portion of a few hours of this type of thing in some other undergraduate course would be an effective thing at least as a beginning and as I say it is going to have to come from pressure outside.

GEORGE CRANSTON: I have a question that is related to the one that was just asked. I want to put it in a little different way I think. We have been told by the educators this morning that we do not have a philosophy of system safety or asking us if we have a philosophy of system safety - that is a legitimate question, but I want to turn the question around after what I have heard and ask them if they have a philosophy of education in our university system and the reason I ask this, from what I have heard it appears that every course is a special course started to meet some special need of some special organization. What we have heard today is the philosophy of that particular course to meet that need, but we have not heard a philosophy about how do we educate people generally in this field.

ANSWER: I think to the common layman it would seem an easier task than it really is to break through the structures at universities. You have to understand the curriculum committees to start with. University curriculum committees are a very strange kind of thing. You approach them with a new idea, no matter how firmly and strongly you believe in it you have to convince them and sometimes they are very hard to convince. It is very true, Mr. Cranston, that these are special interest kind of courses that we have discussed this morning and unfortunately, that is the level we are at right now. I agree with you, we need to do something about that and to motivate. I think maybe an aroused and intelligent public

will do that. Societies will do that if we will continue to motivate people, it might happen.

MR. GROSE: I think you can leave that one open, George, as a rhetorical question.

DR. BALL: This is a comment related to the last question and then a direct question. A couple of weeks ago the National Academy of Engineering held a two day conference on consumer products. Dr. Carl Clark will be speaking on this subject tomorrow and this first workshop was on safety. One of the recommendations that came out of that workshop had to do with the education of the people who are designing and will be designing consumer products such as mowing machines, bicycles, etc. It seems to me that the essence is to teach the design decision-making process. I think it is quite impractical for every aspect of design decision-making to be taught in a separate course so my comment would be that there is a tremendous need in the consumer products area, that the essence is to teach the design decision process, to teach the design and to take into account all aspects of design decision-making including the safety. My question would be to what extent are you teaching the design decision process, have you included safety in this area, not as a special course, not as an option, but simply as an inherent and integral part in the design decision process?

ANSWER: In fairness I think to that question, those present here today are not in the decision making position in the university in order to do that. I think it is one of those things that we are obliged to do though from a professional point of view, to urge that this be done inside university structures. It suffers from all the ills of any bureaucracy I'm sure and it only responds very lethargically to any impulse that comes from society, and I think it is one of those things that conferences like this are essential in proposing as well as professional societies and other people like Ralph Nader. Mr. Nader even has his own way of making himself known but the point is that I agree with what you say, Les, that the decision-making process is sufficiently broad that we cannot afford specialized courses. We do need to focus one more time because the university process has been one of division and separating it to specialties when in actuality I'm sure we need an integrated type of teaching in the universities.

JERRY LEDERER: I have three different comments. First of all, about ten years ago I got the Deans of some of the countries foremost engineering schools together to discuss putting into the curriculars some safety and especially human factors and I was told that there just isn't time. Some universities such as Cornell had increased their engineering course to 5 years to put in humanities as they thought the students should have something on humanities. They had gotten to the point where they are giving them almost entirely engineering. There isn't time, they said, to do this. I would think that at least they could give a couple of electives per semester to get the students thinking about this. The second thing is that we have heard all through this conference that it is the executive who makes the decisions, the businessman. How many universities, if any, have a lecture or two lecturers in their schools of business administration so that you can get the men who become the administrators to recognize there is such a problem. I wouldn't call it safety, I'd call it risk management, part of the management picture. The third item is in connection with the use of system safety for accident investigation. The idea was advanced that you could use those same logic diagrams to conduct the investigation. Also you can use the logic diagrams that were involved in the design to help with the investigation. If you can go back to those logic diagrams, I would think it would facilitate the investigation of an accident enormously in many cases, where structural problems are concerned or systems problems come up, failure of systems and things like that.

QUESTION: I'm not sure that there is such a thing as a non-Government-related industry any more, but if there is such a thing, is there any indication that this side of industry is accepting the concept of system safety as well as the educational side and providing opportunities in form of jobs and salaries that would lure the people from engineering into the system safety side of the house?

ANSWER: I'll respond and I don't know of any. I would just simply say this. I am reasonably certain that the recent emphasis on product reliability is causing the civil sector of the economy to respond to the idea that there are risks that must be addressed and our experience in our particular course is that the students attending from other than aerospace or military part of the economy say that there is a ground swell. It may not be great yet, but it is perceptible and I think we are going to see increasing interest in that area.

COMMENT: I have an observation, I recently read a report that the President of Honda Motor Company that makes the automobiles in Japan has been accused of murder due to reported 16 or 17 deaths which supposedly are due to a design deficiency in the automobile. They are accusing the President of that Company of murder. Obviously, Japan has kind of a strange legal system but those kinds of activities might motivate the consumer product people to respond.

JOHN FRENCH/MSC: I'd like to make one comment. In keeping abreast of system safety activities it would appear appropriate that you visit some of the NASA Centers. I'll speak for Manned Spacecraft Center specifically because we have been involved in system safety from a management and engineering technique standpoint. I would like to welcome any of you gentlemen to come down and discuss these things with us.

C.O. MILLER: Vern, addressing the last two questions, I might mention a visitor we had at the Board a couple of weeks ago. He was a Professor of Engineering from a Midwest University. He had never heard of the term "System Safety" and frankly I don't really know what prompted his visit other than he said, "I've been worried that our people have been coming out of the engineering schools without an appreciation for the hazards that can be designed into a program." I then broke into my standard three-hour lecture on system safety. The point is, I think there is an awareness, well outside the DoD environment on this particular problem as typified by this man. What I gained from it, and I would offer a challenge to not only you on the stage but the people in the audience, I wonder why we don't go back in our memories to our undergraduate days and say for example in aeronautical or say an aerodynamics course, how would we go back to our professor and say, where could you in this course, within its existing framework, introduce some thoughts about system safety?

I submit that I could do this. I could go back in and talk to them about stall spin accidents and where in his course, just as he teaches it today, in an analytical sense or any of a number of other ways, he could come up and engender a feeling in this undergraduate that you ought to look at the hazards. I believe every single one of us, if we chose to, could go back into our own undergraduate field and introduce ideas like this but it is a monumental task.

MR. GROSE: Do you have a practical way, Chuck, to suggest how this might be done. Should we all go back to our own schools as alumni?

MR. MILLER: I think it would be a tremendous challenge to the system safety society to do just this on a local basis.

MR. SHAW/TRW: One of the means obviously of broad education is availability of the literature. Most everyone in the engineering game recognizes it gets obsolete pretty quick and it is a habit of most of the brotherhood to read widely. Coupling that with the idea of the old academic principle of publish or perish, I'd like to raise the question, do any of you gentlemen know of texts available or being prepared at this time on the general subject of system safety?

MR. GROSE: Willie Hammer who spoke yesterday morning is writing a book about it. Willie's book, he tells me, is within 9 months of publication. I have reason to believe there are other books in the mill but I don't have dates.

MR. HOLT: I would like to get a plug out of this. In collaboration with Mr. Richard L. Reeb, who is system safety manager of McDonnell-Douglas Astronautics in Huntington Beach, California, he and I, he is writing a management section and I am writing an engineering section, we're trying to write a book. We don't have any dates but we've got quite a few pages together now -- it's looking good.

COMMENT: I might add one thing too, Bill Rogers at TRW has one in preparation. I have no idea of the date there either.

R. ALTGELT/EATON CORPORATION: I would like to know whether there is a science we might call safety economics that would say, to put it into example form, that one accident would take on the average one-man life and we could show that in the course of a year say X men's lives are taken by this typical accident occurring, and we could show that it would take Y-men's lives of people who are working in factories to eliminate this or eliminate a percentage of this. So far I have been dodging the dollar aspects of it and I recognize a man's life snuffed out isn't the same as the man-life consumer in the shop to add another aspect, conceivably there would be some man-lives that would be lost in industrial accidents producing this apparatus; but I'm wondering, then of course the insurance companies would come in and assign a dollar value to the man-lives and premiums that they have to put out and industries could perhaps be faced with law suits, which could be assigned a dollar value. I'm wondering if there is a science that approaches safety in this way, dollars loss versus dollars spent to prevent, or lives lost versus lives spent to prevent?

ANSWER: I would think that all of our courses try to take this approach. Basically, we try to show the economics whether we are talking about designing a system or probably the specific course would be in our industrial safety-type courses where we talk about cost of accidents, accident elimination and budgeting for safety. I think this is our philosophy inherent in all of our courses. It's the name of the game, really.

SESSION IV

REQUIREMENTS AND MANAGEMENT

Session Chairman - Mr. Charles W. McGuire

"Contracting for System Safety"	Dr. Leslie W. Ball
"Requirements for Systems Safety Programs as Delineated by MIL-STD-882"	Mr. C. O. Miller
"Integrating System Safety into the Basic Systems Engineering Process"	Mr. John W. Griswold

N72-25923

CONTRACTING
FOR
SYSTEM SAFETY

Dr. Leslie W. Ball
Director of Safety

NASA

Marshall Space Flight Center

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

This paper is concerned with those requirements for safety that are, or should be, part of the hierarchy of contractual relationships between government and prime contractors, prime and subcontractors, and subcontractors and vendors.

Each of these interfaces involves the contractual sequence of

1. Request for proposal (RFP's)
2. Proposal documents
3. Contractor selection
4. Contractor performance measurement
5. Fee adjudication

Safety requirements are, or should be, a significant factor in all five of these aspects of the buyer-seller relationship.

The National Aeronautics and Space Agency, the Department of Defense, and most aerospace prime contractors have already a surfeit of policy statements and general specifications that require that safety should be a significant factor in their contracting practices. The purpose of this paper is neither to add to nor to summarize these policy and specification requirements. Rather, our purpose is to invite attention to some of the ways in which traditional contracting methods fail to give confidence in the achievement of safety and then to show how modern system engineering and system management techniques have provided us with the means to overcome these shortcomings in our traditional contracting practices.

OUTPUT CONTRACTING

Let us start our discussion by recognizing two very popular sayings. These sayings have typified supplier attitudes ever since the birth of aerospace industry. They are "Tell me what you want, don't tell me what to do" and "Once the contract is signed, leave me alone until I am ready to deliver the product." Government documents use the term "disengagement policy" to describe this seller attitude to the buyer-seller relationship. Figure 1 "Conditions For Output Contracting" sets forth four conditions that must exist if this type of relationship is to be acceptable to the buyer.

The term "Tangible Characteristics" will be used for those product characteristics that meet the first two conditions shown in Figure 1. For example, in the case of an automobile, top speed, miles per gallon, turning radius, and trunk capacity are tangible characteristics because they can be specified quantitatively and they can be demonstrated by quantitative test.

The term "Intangible Characteristics" will be used for those product characteristics that either cannot be specified quantitatively or, if specified, cannot be measured within acceptable cost and schedule constraints. In the case of an automobile, the intangible characteristics include safety and to some extent the characteristics of operational reliability and quality. In the case of a complex aerospace system, the intangible characteristics may include many other characteristics, such as electromagnetic compatibility or storage reliability.

When all the essential characteristics of a product are tangible, output contracting is the prefered method of contracting from the point of view of both the buyer and the seller. Obviously this is so, because it minimizes the time and effort required by both parties to negotiate and to monitor the fulfillment of the contract. However, even when all essential characteristics are tangible, development risks may make the seller unwilling to forego payment until he has developed the new product and demonstrated that it meets all the specified characteristic requirements. For example, in the case of most missile and space systems, United States aerospace companies are neither willing nor able to forego payment until they have developed a new system, even if all the essential characteristics can be specified and demonstrated by test.

Quite often in the aerospace industry, the customer is unable to meet the fourth condition shown in Figure 1. For example, in the case of the atomic bomb, the intercontinental ballistic missiles, or the Apollo space program, failure to meet all the essential product characteristics within the defined development time would have meant a national disaster.

In summary, we may say that pure output contracting often is unacceptable either because certain characteristics of a product are intangible or because either the seller or the buyer

cannot tolerate some of the risks that are inherent in developing a complex new product.

INPUT CONTRACTING

Let us ask, if it is not possible for a buyer and a seller to contract solely on the basis of defining and demonstrating the characteristics of the product, what then can be done. The only choice is for the buyer and the seller to supplement output contracting by defining the work that the seller will do and paying for the accomplishment of this work. We will call this type of arrangement "input contracting."

A precedent for input contracting was established long ago when the government contracted with universities for research. It is inherent in the nature of research that the product cannot be defined and certainly cannot be guaranteed. Consequently, the agreement between the buyer and the seller is for a defined effort which the seller will make in fulfillment of the contract.

An oversimplification of input contracting would be to say that it consisted of negotiating program plans and monitoring the compliance with the execution of these plans as a condition for payment of the contract costs.

CONTRACTING FOR SAFETY IN THE 1960'S

During the 1960's, several relatively intangible characteristics became of vital importance to the customer. Some of the most important of these characteristics were reliability, maintainability, safety, electromagnetic compatibility, and security.

For each of these characteristics, an effort was made to apply the principles of output contracting. For example, several of us were involved in helping develop the first Department of Defense policy on reliability. This policy oversimplified the problem of contracting for reliability by stating bluntly that quantitative values would be specified in all procurement contracts and that they would be demonstrated before the product was accepted by the government. By the time that contracting for the intercontinental ballistic missiles came along, it was recognized that output contracting was inadequate because condition three in Figure 1 was unacceptable to aerospace industry and that condition four was utterly unacceptable to the government agencies. Consequently, input contracting in the form of requirements for the negotiation, execution, and auditing of reliability program plans developed as a supplement to specification and demonstration of quantitative reliability values.

In the case of safety, there were some initial efforts to apply output contracting by specifying accident probabilities and requiring demonstration of these probabilities by quantitative analysis. However, the limitations of this approach soon were recognized and during the 1960's, contracting for safety was dominated by requirements for safety program plans. These requirements did lead to the growth of a substantial system safety engineering profession. In this author's opinion, many of the members of this profession together with the program plans that they wrote and executed did achieve substantial good. However, a realistic assessment of the current situation must include the criticisms set forth in Figure 2 "Criticisms of Specialist Program Plans."

In general, safety program plans are written by system safety specialist engineers in the contractor's organization to satisfy their professional colleagues in the government agency's organization. In the opinion of many designers, the writing and execution of these program plans has no real impact on their design decisions, and in the opinion of many program managers, these plans have no real impact on their program management decisions.

In the present atmosphere of severe cost reduction throughout the aerospace industry, all specialist engineering staffs are vulnerable. In particular, system safety staffs are being and must be reduced from the levels that existed in the late 1960's.

A relatively new factor has been brought out within the National Aeronautics and Space Agency by the deliberations of the McCurdy Committee on procurement practices. Some members of this committee have pointed out that government specialist engineers, such as system safety engineers, tend to tell the competing contractors so exactly what they require in a program plan that the resulting

proposal documents are essentially identical. Consequently, a source evaluation board is not able to establish discriminators between competing contractors on the basis of their safety or other specialist engineering program plans.

CONTRACTING FOR SAFETY IN THE 1970's

During the first sixteen months of the 1970's, there has been a marked trend away from a multiplicity of specialist engineering program plans and toward the five basic function program plans shown in Figure 3. Continuance of this trend will result in contracting for safety and other intangible characteristics being performed in a manner represented by Figure 4 "Safety Inputs To Contracting." Let us now use Figure 4 as a basis for discussing safety inputs into the five steps in contracting shown in the left hand column.

STEP 1 - REQUEST FOR PROPOSAL

From the point of view of the system safety engineer, the essential elements of even the most voluminous request for proposal are as follows:

1. Product Specifications which define quantitative requirements for the tangible characteristics and qualitative requirements for the intangible characteristics of the product which is to be developed.
2. A Statement of Work delineating the development activities that the buyer considers must be performed by the seller to give confidence in the achievement of both the required tangibles and the required intangible characteristics.
3. Proposal Data List delineating the development program planning data that all the seliers must submit to support the source evaluation and contractor selection processes.
4. Performance Measurement Data List delineating the development program control data that the successful contractor must submit during the execution of the contract.

Item 1 in this list corresponds with the Product Specification column in Figure 4. Items 2, 3, and 4 correspond with the five Basic Program Plans columns shown in Figure 4.

Safety inputs to the product specification inevitably include a motherhood type statement that safety must be a primary consideration in design. However, these inputs can include quite specific requirements such as control of materials flammability, or the use of redundancy to control single point failures for catastrophic hazards. Design practices criteria, in the form of checklists based on experience retention, are applicable to assuring the adequacy of safety engineering inputs into the Product Specification segment of the request for proposal.

The Program Management Plan should be written by the contractor's program manager. It should be a first person description of how he will use his authority and his program management techniques to assure achievement of all the product characteristics set forth in the Product Specification. Specifically, it should describe how he will make use of specialist engineers to help assure that design decisions are right the first time and also to assure that design errors are detected and corrected at the earliest possible time. For example, it should discuss the role of safety analysis in guiding design decisions and participation of safety engineers in design review and development failure analyses.

The Manufacturing Plan should be written by the contractor's manufacturing manager. It should include descriptions of how he will assure achievement of operational safety in the factory and how he will use people such as manufacturing planners and quality engineers to support hazard identification and hazard control.

The Support and Use Plan should be similar to the Manufacturing Plan in that it also should describe how the support manager will assure operational safety and how his quality assurance engineers will contribute to hazard control.

The Integrated Test Plan should bring together in one document an account of development testing, design verification testing, receiving inspection testing, manufacturing check testing, quality acceptance testing, and so on through operational checkout testing.

It should include descriptions of how appropriate supervisors will assure both the safety of the personnel conducting the test and protection of the operation equipment from the stresses that may be imposed during testing.

STEP 2 - PROPOSAL DOCUMENTS

The same safety criteria, set forth in checklist form, which the buyer requires for writing the request for proposal, are needed by the seller for responding to these requirements with his Proposal Documents. The specification segments of his proposal should show how the design that he intends to develop will be capable of achieving all the requirements including the safety requirements.

The program plan segments of the seller's proposal should first describe the resources that he has available for performance of those critical activities that are either set forth in the request for proposal or proposed by the seller himself. In this context, the term "resources" includes the procedures, such as safety analysis procedures, the supporting data, and the available qualified people, such as professional safety engineers. The seller's Program Management Plan should show how his development program organization will facilitate communication between specialist engineers, such as safety engineers, and the design and program decision makers. Each of the other program plans should deal with hazard identification and control activities that are appropriate to the basic function covered by the plan.

STEP 3 - CONTRACTOR SELECTION

Let us distinguish between two extreme cases. In the first case, the buyer has told the seller in the request for proposal precisely what he wants done in each area, such as the system safety area. This means that the buyer has identified all the critical activities that he wants to be performed during the development program. In this case, the only basis for contractor selection is to evaluate the potential effectiveness of the resources that the seller is offering relative to each critical activity. This type of request for proposal has been a major cause of the fifth criticism shown in Figure 2.

In the other extreme case, the buyer has not told the seller what critical activities he wants to be performed; however, he has asked the seller to propose such activities. For example, he may ask the seller to propose such activities. For example, he may ask the seller "What has been your experience in regard to the achievement of system safety? What activities do you propose to perform?" In this case, the source evaluation process must give credit to the seller's identification of appropriate critical activities as well as to the resources that he proposes to put to work to accomplish these activities.

STEP 4 - PERFORMANCE MEASUREMENT

For the tangible characteristics, performance measurement is dominated by qualification testing and system testing. These tests demonstrate that the quantitative values required by the product specification have been achieved by the seller's design.

In the case of safety and other intangible characteristics, quantitative performance measurement is almost meaningless. Consequently, criteria must be established for evaluating the performance of the critical activities set forth in the five basic program plans. The key to accomplishing this objective is illustrated by Figure 5. Modern system management requires that all the work to be accomplished during a development contract be related to a single Work Breakdown Structure. Cost Accounts are formed by matrixing the work breakdown structure with the contractor's organization units. Work Packages may be formed in several logical manners. This chart illustrates the formation of work packages by dividing the work to be done by a particular organization on a particular work breakdown structure item into short duration packages.

The vital management requirement illustrated by Figure 5 is that critical activities, such as safety analyses, must be specifically required and scheduled and funded by their inclusion in the Work Package Work Description. Also, satisfactory completion of the critical activities must be provided for by inclusion of tangile criteria in the Work Package Closeout Criteria. For example, such criteria must be

2-5

established for the accomplishment of each type of hazard identification analysis and for each type of hazard control activity.

STEP 5 - FEE ADJUDICATION

From the point of view of the customer's system safety manager, the award fee type of contract is by far the most attractive. This type of contract provides incentive for the buyer and the seller to agree on what should be done during each award fee period of, say, six months. If the total award fee is to be in the range from two to fifteen percent, it is reasonable to assign, say, one-half of one percent to the accomplishment of the safety program. It is this tie-in between the performance of safety activities and award fees that provides the best hope for full exploitation of the skills, knowledge, and techniques of the professional system safety engineering during the 1970 decade.

SUMMARY

In summary, the safety contracting methodology of the 1960's was dominated by individual safety program plans together with a need for large and expensive system safety staffs to prepare, execute, and audit the execution of these plans. During the 1970's, there is a rapid trend toward the absorption of system safety disciplines into the five basic function program plans. The contracting practices of both the buyer and the seller should reflect and encourage this trend. In particular, the award fee principle should be used to provide confidence that system safety technology will be fully exploited during the 1970's.

BASIC FUNCTION PROGRAM PLANS

- PROGRAM MANAGEMENT PROGRAM PLAN (PHASE A, B OR C/D)
- SYSTEM ENGINEERING PLAN (MIL-STD-499 SEMP)
- MANUFACTURING PLAN (INCLUDES FACILITIES AND QC)
- SUPPORT AND USE PLAN (INTEGRATED LOGISTICS SUPPORT)
- INTEGRATED TEST PLAN

SPECIALIST ENGINEERING CRITICAL ACTIVITIES MAY BE DELINIATED IN SEPARATE PLANS BUT THEY MUST ALSO BE INTEGRATED INTO THE ABOVE.

FIGURE 3

SAFETY INPUTS TO CONTRACTING

- CRITERIA REQUIRED EITHER TO HELP WRITE OR TO HELP EVALUATE THESE ITEMS

	BASIC PROGRAM PLANS					
	PRODUCT SPECIFICATIONS	PROGRAM MANAGEMENT	SYSTEM ENGINEERING	MANUFACTURING	SUPPORT AND USE	INTEGRATED TEST
REQUEST FOR PROPOSAL	•	•	•	•	•	•
PROPOSAL DOCUMENTS	•	•	•	•	•	•
CONTRACTOR SELECTION	DECISION BASED ON EVALUATIONS					
PERFORMANCE MEASUREMENT	•	•	•	•	•	•
FEE ADJUDICATION	DECISION BASED ON EVALUATIONS					

FIGURE 4

CONDITIONS FOR OUTPUT CONTRACTING

- ALL ESSENTIAL PRODUCT CHARACTERISTICS CAN BE SPECIFIED QUANTITATIVELY.
- ACHIEVEMENT OF ALL CHARACTERISTIC CAN BE PROVED WITHIN ACCEPTABLE COST AND SCHEDULES.
- SELLER IS WILLING TO FOREGO PAYMENT UNTIL ACHIEVEMENT OF ALL CHARACTERISTICS HAS BEEN DEMONSTRATED.
- BUYER CAN TOLERATE THE SCHEDULE AND COST IMPACT OF CANCELLING THE CONTRACT FOR NON-PERFORMANCE AND STARTING AGAIN WITH A NEW SUPPLIER.

CRITICISM OF SPECIALIST PROGRAM PLANS

- WRITTEN BY SELLER SPECIALISTS TO SATISFY BUYER SPECIALISTS
- NO REAL IMPACT ON DESIGN DECISIONS
- NO REAL IMPACT ON PROGRAM DECISIONS
- REQUIRE LARGE STAFFS TO WRITE, EXECUTE AND AUDIT
- NO DISCRIMINATION BETWEEN COMPETING SELLERS

FIGURE 2

TECHNICAL ASSURANCE THROUGH CSTCS

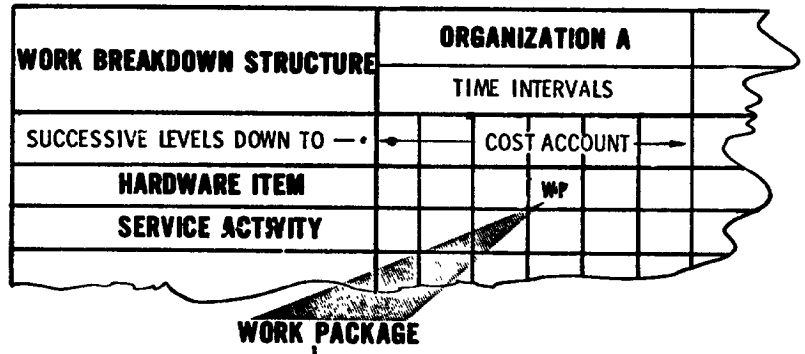


FIGURE 5

REQUIREMENTS FOR SYSTEMS SAFETY PROGRAMS AS DELINEATED

BY

MIL-STD-882

Dr. C. O. Miller, Director
Bureau of Aviation Safety

National Transportation Safety Board
Department of Transportation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

FOREWORD

As part of the Second NASA Government-Industry System Safety Conference, this paper was prepared to inventory the development and features of the currently best known system safety requirements document, MIL-STD-882, "System Safety Program for Systems and Associated Subsystems and Equipment...," dated July 15, 1969. NASA officials requested me to prepare it and, although I have not been in mainstream Department of Defense (DOD) efforts to implement the standard recently, I was in an active advisory capacity to DOD during the Standard's formulation and, indeed, its predecessors, the MIL-S-38130 series. Presumably, this would provide a degree of objectivity at least in assessing the successes - and failures - of the Standard thus far.

Unfortunately, this is not necessarily the case. I remain biased! I firmly believe there is a need within the management work structure of any reasonably complex system for a defined and implemented system safety program. The "whys" of this need have been chronicled elsewhere by others as well as myself. In any case, some implementing process is required.

As a result, this paper merely reiterates certain development history of MIL-STD-882 and attempts to spell out the role of the Standard through, among other ways, identifying its norms, its strengths, and its weaknesses. Further, of course, there are some considerations for the future.

This paper is not to be construed as representing an official position of the National Transportation Safety Board although the record has clearly shown the Board's endorsement of the system safety concept.

C. O. Miller

N72-25974

REQUIREMENTS FOR SYSTEM SAFETY PROGRAMS AS DELINEATED BY MIL-STD-882

EVOLUTION OF SYSTEM SAFETY PROGRAM REQUIREMENTS

In January 1946, Amos L. Wood of the Boeing Company presented an Institute of Aeronautical Sciences (IAS) paper regarding a recommended air safety program for aircraft manufacturers. He emphasis "continuous focus of safety in design... advance analysis and post accident analysis... accident preventive design to minimize personnel error... safety work, most effective when it is not fettered by administrative organizational pitfalls." (1)*

In February 1948, William I. Stieglitz wrote:

> "Safety must be designed and built into airplanes, just as are performance, stability and structural integrity... Every engineer cannot be expected to be as thoroughly familiar with all the developments in the field of safety anymore than he can be expected to be an expert aerodynamicist... (thus) A safety group must be just as important a part of a manufacturer's organization as a stress, aerodynamics, or weights group... (although) A safety program can be organized in numerous ways and there is probably no one best way." (2)

While the obscurations inherent in history preclude totally accurate revelation of who said what to whom first, these quotations represent the two earliest statements of what can be considered the cornerstone system safety principle. Namely, that at some level of system complexity, management is most effective and efficient if it were to require a specialized approach to safety as well as safety being simply everyone's job.

That this has come to pass is not a matter of argument, it is a matter of record. (3) The military services implemented this philosophy in their operational segments in the early 1950's. In this same time frame, many aircraft manufacturers established flight safety engineering groups (and without government requirements!). The aircraft complexity barrier was being faced and a number of ility functions were being called upon to supplement heretofore normal management division of work to provide a functional, economical, reliable, maintainable, available and sufficiently safe system so that a mission could indeed be performed.

Then, in oozed systems management. This not only called for a life cycle look and a better description of what comprised a system, but it produced a plethora of contractural documents.** Missile and space vehicle development in the late 1950's required this approach not only because of the aforementioned complexity problem being carried over and amplified from aircraft development, but also the loss of a single vehicle became an economic and mission degradation that simply would not tolerate less than an all out accident prevention effort. And the mood of the times dictated more clearly defined documentation during the engineering phases, including safety programming, as it had been implemented a decase earlier in the aviation operational world.***

Highlights of such specification predecessors to MIL-STD-882 are summarized below:

MIL-S-23069 (WEP) "Safety Requirements, Minimum, for Air Launched Guided Missiles" October 31, 1961

> This oft forgotten document broadly identified life cycle requirements for a system safety program. Its implementation, however, was minimal, at

*Number in parenthenses refer to references noted at end of paper.

**An interesting analogy is possible here. "Plethora" is defined in the medical sense as "a disease caused by an excess of red corpuscles in the blood or an increase in the quantity of blood in the body." This led one writer to observe" ...a person in plethora (is) dying from too much health" (Sheridan as quoted in the World Book Encyclopedia Dictionary, 1963). Consider the "health" of the aerospace industry today... too much documentation???

***It has also been argued, perhaps not too facetiously, that in missiles, you no longer have a pilot to blame for the vehicle's loss, so why not go further upstream to the system's design?

least at its beginning. The Navy organization then, as now, was not conducive to life cycle system safety implementation efforts.

BSD Exhibit 62-41 "System Safety Engineering: Military Specification for the Development of Air Force Ballistic Missiles" June 1962

This USAF Ballistic Systems Division document was noteworthy on several counts. First, it was the initial definitive system safety specification that was implemented in major aerospace programs. Almost of equal significance, it was the first time such an engineering effort received the unqualified support of the head of the procuring agency who literally directed BSD contractor management personnel to get with the program, so to speak, or forget doing business with BSD. (4)

MIL-S-38130 (USAF) "General Requirements for Safety Engineering of Systems and Equipment" September 1963

Actually, Commander Donald Layton USN made major attempts to translate BSD Exhibit 62-41 into a broader based system safety engineering specification applicable to all DOD aerospace systems. However, he encountered in-house resistance by the BuWeps Industry Material Reliability Board which preferred to wait for a broader program that would encompass safety, reliability, maintainability and other similar requirements under one heading. (5) Concurrently, Lt. Col. James McConnel of the USAF Systems Command Headquarters aggressively shepherded the document through Air Force channels as a cleaned-up version of BSD 62-41. What it contained was basically four requirements:

(1) A safety management program
(2) Criteria to produce a reasonable level of safety
(3) Hazard analysis
(4) Program milestone reporting

MIL-S-58077 (MO) "Safety Engineering of Aircraft Systems, Associated Subsystems and Equipment; General Requirements for" June 30, 1964

This Army specification was a virtual verbatim issuance of MIL-S-38130. Interestingly enough, the Army was the first service to apply its specification to a new aircraft program, the Armed Aerial Fire Support System (AAFSS). (6)

MIL-S-38130A (DOD) "System Safety Engineering of Systems and Associated Subsystems, and Equipment, General Requirements" June 6, 1966

In the 1964-5 time period the Air Force Systems Command (AFSC) continued leadership in system safety by not only requesting an updating of MIL-S-38130, but also developing a System Safety management guide and a System Safety design handbook (ultimately published as References 7 & 8). Concurrently, a decision was made to implement the system safety approach DOD-wide as part of a continuing program of interservice standardization of requirements documentation. (9) AFSC was named Office of Primary Responsibility (OPR) for the task. The result was MIL-S-38130A (DOD). It subsequently was introduced into many programs both new and underway.

At this point the reader might ask "why all this discussion on the history of system safety and particularly the specification and current standard development?" The answer is so simple as to often be overlooked by the newcomer to system safety and MIL-STD-882. There is a decade or two of specific technological and managerial experience that has shaped MIL-STD-882, time which has demonstrated the need for such a programmed approach, time which has seen senseless waste of men and other resources that could have been avoided by an improved systems approach to safety.

Does this mean MIL-STD-882 is a model document? Far from it as will be discussed subsequently. It simply means some very astute and high ranking management types, both inside and outside the government, had fully adopted the system safety principle by the time the decision was made to go to a "standard." Indeed, the combined talents of many people offered a check and balance into

what had preceded the standard and what got into the standard itself.*

MIL-STD-882... ITS CHARACTERISTICS

Like any Military Standard, MIL-STD-882 must be considered as the uniquely defined type of document that it is. For example, a Military Standard does not connote the preciseness of every yardstick being 36 inches long. Nor does it connote some minimum acceptable level of performance as is generally the case with "standards" issued by the Federal Aviation Administration. A standard is, by DOD definition, as follows:

> "A document that establishes engineering and technical limitations and applications for items, materials, processes, methods, designs, and engineering practices. (10)

Engineering standards, further, are "documents created primarily to serve the needs of designers and to control variety... define terms, establish codes and document practices, procedures and items selected as standard for design, engineering, and supply management operations." (11)

Military standards are not to be used as the direct medium for imposing administrative requirements on contractors. Rather, standards function in procurement through the medium of specifications. (12) Specifications are in turn defined as:

> "A document intended primarily for use in procurement, which clearly and accurately describes the essential technical requirements for items, materials, and services including the procedures by which it will be determined that the requirements have been met." (10)

Accordingly, MIL-STD-882 is more a guide than a directive at least until program management decides to follow it. Then it becomes a matter of further delineation, through specifications or otherwise, to implement a specific program tailored to the system under consideration including where that system is in its life cycle.

To be more precise in what MIL-STD-882 comprises, consider it in two ways: first, the problems inherent in MIL-S-38130A which were corrected and, second, what are the Standard's basic features.**

During its application, MIL-S-38130A was revealed to be limited if not dificient in that it:

(1) Did not adequately define terms necessary for its understanding.
(2) Was limited to the engineering phase of the life cycle only thus negating optimum effectiveness of total system safety management practices.
(3) Entailed excessive emphasis on the analytic process to the exclusion of other tasks.
(4) Produced further confusion between safety and reliability engineering efforts particularly because of a failure to delineate between the two in the analytic process.
(5) Failed to acknowledge the role of training in the accident prevention process.
(6) Failed to provide for safety data communication and interchange between the customer and contractor and within the customer's own organizational segments.
(7) Failed to provide for a safe and acceptable disposal of equipment and material at the completion of their usefulness.

*Not to be forgotten in this entire discussion are other events in the evolution of system safety such as the direction of the concept into the SST program by the FAA in 1965, the Apollo 204 fire that launched NASA into system safety, the National Transportation Safety Board's recommendations regarding system safety in surface modes of transportation, etc. While not directly bearing on MIL-STD-882, these non-DOD developments in system safety are further testimony of the acceptance of system safety principles.

**It can be argued that MIL-S-38130A was neither specific enough as a specification nor sufficiently encompassing as a standard. Another reason for establishing the standard was the desirability to place in the documentation hierarchy a top document under which various detail system safety specifications could develop logically.

As will become apparent in a moment, these shortcomings were corrected for the most part in the published MIL-STD-882.

Like all military standards, of course, MIL-STD-882 is couched in governmentese language. However, when all the confusion factors are eliminated, what the document really says is this:

(1) It tells why the standard is in existence, i.e., to provide for a system life cycle program for safety with the planning function being used as the overview control document. Observe this goes well beyond engineering per se... a fact often not recognized by the casual student in the field.

(2) It defines terms which, in their finality, look simple. In actual fact, however, they bear careful study. The nuances existent in the use of the word system (rather then systems) or the need to distinguish between different levels of contractors are but examples of where meanings must be fully appreciated before many other parts of the standard fall into place.

(3) It provides requirements within constraints present in any "standard" type document as discussed earlier. These include:

a. A System Safety Program Plan (SSPP).
b. Specific tasks in different phases of the life cycle.
c. An explanation of what safety organization is present to implement the program.
d. Milestone and program review points.
e. Detail consideration of hazards and the analysis thereof, to include corrective action or control processes available.
f. Safety data production and interchange.
g. Testing considerations, both in verification of given safety performance and insuring test programs being performed safely.
h. Training program inputs.
i. Special consideration of ground storage and handling problems including system close-out requirements.

(4) It provides, albeit brief, a relationship to associated disciplines, particularly to system engineering.

In addition, the sample System Safety Program Outline (Appendix A to the Standard) infers other tasks that might be expected within the scope of an SSPP, e.g., accident investigation planning and procedures, audit programs, establishment of system safety groups, etc.

In summary, MIL-STD-882 is a document which says "You ought to consider a system safety program, plan for it, and here are some of the prime considerations when you do." It is the basis for good dialogue with management when they face their difficult decisions about safety. It is the system safety practitioner in his relationship to management what the blueprint is to the designer in his relation with his management or with the manufacturing department.

A long-time colleague, Vernon L. Grose, also put it succinctly this way:

> "A System Safety Program Plan is a mechanism to translate a generalized standard into a language that management understands in terms of cost, performance, and schedule." (13)

Enough said for the objectives and good points. What about the problems with MIL-STD-882? And it does have some, or at least the system trying to use it does!

MIL-STD-882... ITS PROBLEMS

Without attempting any rank order listing, let us consider various adverse comments involving MIL-STD-882 derived from a number of personal interviews and a review of a particularly critical analysis of the standard appearing in the Journal of Quality Technology, October 1970. (14) Before proceeding, however, it is of interest to note that as of May 1, 1971, the OPR for the Standard, AFSC Hdq (IGFS) had not received a single written criticism as requested routinely in all standard documents and appended to each release (DD Form 1426). This followed, among other communications, a specific request for such comments at the USAF-sponsored System Safety Conference in Las Vegas, February 1969.

Nevertheless, listed below are the problems encountered and personal editorial-type views of this author noted under "Comment."

1. The Standard is too confusing... is not easily understood.
   Comment: Perhaps true; however, a standard in safety cannot be expected to be understood or appreciated by persons not well versed in the field any more than a powerplants engineer could be expected to fully comprehend a standard in electromagnetic radiation. In other words, one should know the business before trying to criticize it! Still, the challenge remains to put the Standard in words a broader-based population can grasp.
2. There are minimal numbers of trained and/or experienced personnel in the system safety field and unfortunately non-qualified engineers are often assigned to system safety tasks both at the contractor or at the procuring agency.
   Comment: A very valid point and one closely allied with the previous item. The solution rests not only with more and better system safety literature and training, but also with continued professionalism by those in the field. Further, the pseudo safety expert, (who) got that way because his boss merely told him to put on a system safety hat) must be recognized and exposed for what he is.
3. Each program must have a safety effort delineated for its own peculiar needs.
   Comment: That's correct and as it should be, albeit more ingenuity and hard work may be involved than to simply follow MIL-STD-882 in checklist fashion. But, since when do we accomplish progress in our aerospace field "by the numbers" or, even more importantly these days, do it within reasonable economic limits without ingenuity and hard work?
4. The Standard or other documents do not relate system safety to other disciplines.
   Comment: Another valid point, although the place for such delineation probably does not belong in MIL-STD-882 but rather in something like MIL-STD-499, "Military Standard, System Engineering Management." (MIL-STD-499 is only under trial use today by the USAF.) In any case, the distinctions have been made in various contributions to the technical literature.
5. Duplication of efforts "ilities" or between system safety efforts and designers is encouraged by MIL-STD-882.
   Comment: Even discounting the fact that planned duplication of some effort (e.g. critical hazard analyses) may often be a wise management technique, the problem suggested here has arisen. It does so because contractor and/or customer organizational segments have parochial interests which preclude cooperation between different organizational segments. Or, as covered more in the next item, the documentation requirements are conducive to separate reporting.
6. Information is developed for contract satisfaction rather than for use at the time of its inception or downstream.
   Comment: This may well tie in with the people experience problem described earlier but in any case is considered by many to be the principal problem associated with MIL-STD-882. For example, if timing of hazard analyses are not predicated upon their contributing to the design or their output does not tell a usable story to downstream personnel, what really has been accomplished? Answer: A paper exercise... and it has happened.
7. In contractural arrangements with some parts of DOD a single integrating contractor is not designated thus, making system safety integration a bureaucratic nightmare.
   Comment: A serious problem: As to just how serious, the DOD agencies can only answer for themselves.
8. Implementation of a total life cycle system safety program within most military organizational structures is difficult because of excessive administrative barriers between development and using commands. The arsenal approach simply does not provide for a life cycle approach to anything including safety.
   Comment: This has been a long standing problem which can be overcome to

some degree by formation of a strong system safety group early in the program and not letting it become degraded with time. This would seem to be dependent upon the initiative of operating command personnel even more than those at the development end of the spectrum.

9. System safety cannot be quantified and, therefore, the hazard analyses can never become a part of management's prime effort in maintaining a high benefit to cost ratio for its efforts.
   Comment: This myth continues to surface periodically but fortunately aerospace technology has seemed to come around to the real world pleaded for on this subject by system safety types for many years. Witness DOD Instruction 7041.3, "Economic Analysis of Department of Defense Investments," which states "An economic analysis is not required... when it can be shown that an analysis would not... result in increased decision effectiveness." (15) Actually, the principal contribution of hazard analysis is to make people think before the accident instead of afterwards... not the paper result.
10. System safety costing difficulties are continuing. No one seems to have found an adequate formula for what should be a direct charge, vis a vis an overhead charge, for system safety. Further, all too often, unqualified people at the negotiating table are discussing safety-generated work items.
    Comment: Once again, an old problem but one that is faced by anyone operating at the marketplace today. Resolution would seem best achieved when solution to the next item listed is forthcoming.
11. Safety tasks suggested by MIL-STD-882 are not definitive enough.
    Comment: This would seem to be a valid criticism and will remain so until more "how-to-do-it" technology is documented and understood by all. The design safety handbooks on hand and/or underway by some of the services are a major step in this direction. However, as indicated earlier system safety tasks are not uniquely those associated with design, and the total collection of such material in text form is still on the distant horizon.
12. The feedback loop to system safety of a given system via the accident/incident investigation process does not seem to be well established.
    Comment: As noted earlier, the outline SSPP acknowledges accident/incident investigation as a part of the program. But what about an effective closing of the loop back to the designer, the production man, the manager, etc., of the specific results of the investigation conducted by either the manufacturer or the customer? Is it really being done? Answer: No!
13. The fear of litigation has not only restricted information interchange concerning accident/incident investigations (applies to 12 above) but also has inhibited accomplishment and dissemination of information associated with hazard analyses.
    Comment: Sooner or later all firms and agencies will realize that a far greater risk is incurred concerning their possible culpability if it can be shown they did not use state-of-the-art analytical techniques at their disposal when the product was designed, tested, or turned over to the operator. And such techniques can be described in courtrooms today by any number of qualified consultants. What exists today in this regard is the psychological roadblock in the minds of most technologists concerning anything related to legal proceedings.
14. Several questions about the logic used involving the term "hazard":
    a. Why a "system safety hazard?" (Section 4.2.4 of MIL-STD-882)
       Comment: Does it mean a hazard to safety?
    b. A Category I hazard is called "Negligible," that is, it will not result in personal injury or damage.
       Comment: The question remains if it won't cause injury or damage, how can it be called a hazard?
    c. The Category IV hazard is of most concern.

Comment: Number four out of how many? (Besides, it is the exact opposite numbering logic than that used by NASA, although at one time during discussion regarding the Standard, NASA's logic was the same.

These comments regarding "hazard" approach the nit-picking category but are troublesome questions that could stand some editorial correction.

Observe that some if not most of the basic problems described could be dismissed as being non-relevant to the Standard itself, and, in fact, simply described as faults of the system in which the Standard operates. But let us take a lesson from our own system safety methodology. If something has problems, you do not just look at any single piece of the action to effect corrective measures. You also look at the interrelationships wherever they exist and try to make corrections wherever possible within existing fiscal and time constraints. In the end, then, your individual components start looking better as well as the total system performance.

SUMMARY AND REMARKS

System safety in general and MIL-STD-882 in particular will not remain static since the overall aerospace business will not remain static. The emphasis placed on the evaluation phase of system procurement by DOD is one example of change being felt now.(16) Another is a programmed detailed review of MIL-STD-882 to be performed in the next few months by a committee representing the military services safety centers.

It would seem that during these dynamics, it is encumbent upon the workers in system safety to continue their professionalism and dedication to the accident prevention task. Then, too, the system managers should try to be open-minded enough to try to understand the contribution that can be made by utilization of the principles outlined in MIL-STD-882 albeit they should not be satisfied unless they are convinced a system safety approach contributes positively to their mission. This is something that can only be accomplished by their association with qualified people in the field.

Of all the problems encountered in research for this paper, the item most frequently illuminated was the lack of appropriate people at the decision points where system safety was needed or used. This is not just a matter of education in the sense of people having a general association with the principles of system safety. It is also a matter of a better understanding of the "how-to's" of system safety... the specific safety tasks that must be delineated for a given program, man-loaded in the work allocation process, scheduled with the other work, and assessed as to their effectiveness by measures valid for the tasks that have been performed.

Whoever said "Safety is a responsibility, not a task" was living in a philosophical dream world.(17) You do not achieve accident prevention by just appealing to people's ethical values, you get out and work using proven accident prevention techniques. In this regard, most of the educational programs in existence concerning system safety are just that, education rather than training. The sponsors cannot seem to afford to pay for or allocate the time of their people to have each task subject covered in depth. An exception to this might be thought of in terms of the Fault Tree analysis course at the University of Washington. However, Fault Tree is just one analysis technique among dozens that might be used. There are many tasks besides analysis, and recognizing this, one begins to appreciate the magnitude of the job of training people in the system safety discipline, let alone educating those on the periphery.

Appreciating the above problem, there becomes a need for more manuals and, yes, specifications, when the techniques are reasonably solidified. Another possibility would be a series of Aeronautical Recommended Practices (ARP's) by the Society of Automotive Engineers (SAE) or similar publications by the EIA G-48 Committee.* In any case, the discipline must be documented in every expanding fashion with constantly improving professionalism if it is to compete in the marketplace for management's dollars.

One thing is to have a MIL-STD, and even a series of explanatory directives such as AFSCM 127-1, (7) or the Army's AMCP 385-23, (18)

*Electronics Industries Association, System Safety Engineering Committee, G48.

It is quite another thing to have something quite specific to implement.

Finally, as a major finding of this little study, a question is posed. Do we want paper or progress? All too often in the implementation of MIL-S-38130, MIL-S-38130A, and even MIL-STD-882 thus far, too many people seem to think the objective was to turn in a specified number of documents so that a box could be checked off for contract progress reports. A disproportionate amount of time has been spent figuring out the paper flow compared to expeditious resolution of the dirty details of what the paper contained. Fortunately for all of us, this "easy way out" has not always been the case and things are improving. Ask some of the aircraft manufacturers of those weapon systems to which MIL-STD-882 has been applied.

In conclusion, the two decades or so of effort leading up to MIL-STD-882 has not all been fun and games. Nor will the next two decades be such while we advance man's ability to control those forces of destruction that, in increasing fashion, he himself has created. But we will be working at it.

REFERENCES

(1) Wood, Amos L., "The Organization and Utilization of An Aircraft Manufacturer's Air Safety Program." The Boeing Company, Seattle, Washington. Presented at the Institute of the Aeronautical Sciences Meeting, New York, January 1946.

(2) Stieglitz, I., "Engineering For Safety." Aeronautical Engineering Review, February 1948.

(3) Miller, C. O., "The Role of System Safety in Aerospace Management" University of Southern California, Los Angeles, California, August 1966.

(4) Personal communication with Lt. Col. (Ret.) George Ruff, 1965, (considered by many to be the author of BSD Exhibit 62-61)

(5) U.S. Navy, Letter to the Assistant Chief for Research, Development, Test and Evaluation from the Intra-Bureau Systems Effectiveness Policy Committee, RAAV 02/39, Washington, D.C., April 9, 1964.

(6) Hamilton, Col. R. M., and Capt. R. W. Newton, "The Army Evaluation of MIL-S-58077, and Those Agencies Involved in Its Implementation." Annals of Reliability and Maintainability, Vol. 4 (Washington, D.C.: Spartan Books, July 1965).

(7) U.S. Air Force Systems Command, "AFSCM 127-1, Safety Management" January 1, 1967.

(8) U.S. Air Force, Systems Command, "DH-1-6, System Safety" July 25, 1967.

(9) U.S. Department of Defense, DDR and E Memorandum, "Safety Engineering Requirements for Systems and Equipment - Specification Consolidation and Tri-Service Coordination," August 5, 1965.

(10) U.S. Department of Defense, "Standardization Policies, Procedures and Instructions," (Glossary)

(11) Supra (Paragraph 2-103)

(12) Supra (Paragraph 2-103 and 1-204)

(13) Personal communication with V. L. Grose, April 1971.

(14) Bailey, Peter H. G., and Eugene R. Christie, "Review of Standards and Specifications," MIL-STD-882, System Safety Program for Systems and Associated Subsystems and Equipment" Journal of Quality Technology, Volume 2, No. 4, October 1970.

(15) U.S. Department of Defense Instruction 7041.3, "Economic Analysis of Proposed Department of Defense Investments," February 26, 1969 (Part III B1a).

(16) Letter to DOD activities by David Packard. "Policy Guidance on Major Weapon System Acquisition," May 28, 1970.

(17) As quoted anonymously in the Flight Safety Foundation Aviation Safety Exchange 70-402/403, Arlington, Virginia, 1970.

(18) U.S. Army Materiel Command AMCP 385-23, "Management System Safety," July 1967.

N72-25975

INTEGRATING SYSTEM SAFETY INTO THE BASIC SYSTEMS ENGINEERING PROCESS

Mr. John W. Griswold
Reliability & System Safety Manager

Aerospace Group
The Boeing Company

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

In any undertaking there is always a competition for resources. Decisions must be made for each expenditure of time and money. Functional and specialty groups compete for the funds necessary to do the best possible jobs within their specialty.

No one gets all the money they want and each element of a total system, be it management or technically oriented, must prepare the best possible argument for their position. Dedicated specialist groups are becoming more sophisticated in their approach and have given up on the motherhood approach in favor of hard facts determined from detailed analyses.

The system safety function is no different from other specialist groups in its need to compete for limited resources. Although man is inherently reluctant to settle for less than the ultimate in safety, a program manager is sooner or later faced with the decision as to how safe is safe enough.

The combination of all specialist groups inputs into a balanced program is essential. The systems engineering process is a method that defines the system and its functions, integrates the requirements of all of the subfunctions, sets priorities for funds and time to carry out the tasks and directs the combination of all engineering efforts to complete the program. By definition the system safety effort thereby becomes a part of the systems engineering process.

The term systems engineering has been used to describe many different things. To properly respond to the title of this paper, a baseline description of systems engineering must be established since system safety is one of the subfunctions in the systems engineering process.

Although many of the elements of systems engineering had been applied before, the Air Force -375 (1) series of manuals in 1964 focused attention to combining these elements into an engineering discipline. This series has now evolved into MIL-STD-499 (2), "System Engineering Management," which is taken as the baseline description of the systems engineering process for the purpose of this paper.

The government objectives in MIL-STD-499 are: a) the efficient engineering definition of a complete system; and b) the efficient planning and control of the technical program for the design, development, test, and evaluation of the system. Contractors must provide a logical sequence of activities and decisions leading to the definition of the configuration, usage and support of the system and technical program for acquiring a system. The definitions established by systems engineering provide the basis for the subfunctions to conduct their analyses and establish their requirements on the system. This is an iterative process starting with the conceptual phase and extending through the life of the program. The subfunctions include but are not limited to the following: Design, Test, System Safety, Reliability, Logistics, Maintainability, Quality, Human Engineering, Configuration Control, Security Engineering, and Value Engineering. Other subfunctions may be added for specific programs.

THE SYSTEMS ENGINEERING PROCESS

The basic elements of the systems engineering process are given in Figure 1. Detailed discussion of each of the systems engineering elements are included in MIL-STD-499 and will not be covered here. This paper will address itself to the information that system safety requires from systems engineering, and the information that system safety provides to other subfunctions of systems engineering.

MIL-STD-499 requires and defines the preparation of the systems engineering plan. It is recognized that this is essential to the proper planning and control of the systems engineering program. MIL-STD-882 (3) places a great emphasis on the system safety plan. It requires that one be prepared for each Department of Defense Program. NASA NHB 1700.1 - Vol. III (5) also specified that a system safety plan be prepared for each project or program.

The proper preparation and integration of these two plans is of utmost importance. After they are approved by management they become the controlling documents for systems engineering and system safety. It is in the

system safety plan that the necessarily general requirements of a specification or program guide are merged with the specific needs of a particular program to define tasks and responsibilities to make a safety program live and breathe.

SYSTEM SAFETY PROGRAM

System safety has gone through many of the same growing pains as systems engineering. The need for improved product safety was recognized and the only way to assure it was to consider the entire system. The problems of definition, purpose, scope, and charter of system safety were pounded into shape until there is now general acceptance of the system safety discipline. MIL-S-38130 was published and later revised to MIL-STD-882. That, combined with the NASA SPD-1 (4) and NHB 1700.1 series, provides all of the baseline and direction necessary for a system safety program. Vern Grose offers a definition for system safety (6) that illustrates its pervasiveness with the systems engineering process (see Figure 2).

The successful and cost effective implementation of the safety program requires information to be available or developed. The results of the safety analyses and other efforts must flow to other organizations to become useful. Figures 3-8 show a simplified flow of a typical system safety program. The sections that follow will discuss this flow of information, how it is used by system safety and how the rest of the systems engineering subfunctions are affected.

The basic tasks of any system safety program can be grouped into four basic headings: 1) the assembly of information and data; 2) the analysis of that information and data to determine the hazards to the system and the probability of the hazards resulting in accidents; 3) the establishment of preventive measures through requirements and standards; and 4) a follow-up activity that assures the requirements and standards are included in the design and operation of the system and that they are adequate. Ideally, the tasks should be started at the conceptual phase and upgraded throughout the life cycle, through an iterative process, improving the system as more information becomes available.

Information and Data (See Figure 9)

It is obvious that no work can start until there is some kind of system description. This is the start of the systems engineering process and one of the most important elements. The description must be as complete as the program phase allows; it must be published to all functional elements; it must be revised as necessary and all subfunctions must be kept aware of the revisions. This description must include the hardware, its intended use and the environment in which it is intended to operate.

The initial system description allows system safety engineers to start to assemble experience retention information and data to prepare for the analyses and trade studies that may be needed. Information from past and current programs can provide the basis for the initial safety criteria and guidelines that should be provided to the systems engineers and designers. Range safety documents, government standards and codes and documents such as the Air Force System Command Handbook DH 1-6 (7) are sources for much of the initial information needed. The experience retention data accumulated by other subfunctions should also be made available in a data center to avoid duplication of materials. Reliability, maintainability and human factors experience data must also be considered by system safety.

Preliminary system safety requirements can be established from this initial data. For example, ordnance design requirements are well established and can often be taken directly from past programs. The use of fuels and propellants may require ignition proofing or explosion proof equipments. Nuclear power sources require special shielding and handling. These and many other obvious requirements are provided to systems engineering to be included in the systems requirements. It is also advisable to start a system safety requirements document that can be used as a checklist during design reviews, flight readiness reviews and audits.

System Safety Analyses (See Figure 10)

The systems engineering inputs given on Figure 9 must be available to allow a complete and effective safety analysis. The system description, functional flows and time line analysis must be current and controlled by configuration control to assure that all subfunctions of systems engineering are considering the same system.

The system safety analyses must: a) identify the hazardous elements, hazardous conditions and potential accidents that could occur; b) determine their potential effects on the system; c) determine the probability of their occurrence (qualitative or quantitative); and d) provide adequate detail to direct the corrective action necessary to control the hazards to an acceptable level.

Mission goals and objectives must be considered in the emphasis given to system safety. A much higher risk may have to be taken in a weapons system with a high priority for early use than would be acceptable on a manned space station. The system safety function, along with others in the systems engineering process, must identify levels associated with trades against cost, weight, functional capabilities, and other system constraints.

The system requirements of other subfunctions must be known to system safety engineers so they can be considered in the safety analyses. More will be said of requirements later. The reliability, maintainability, logistics, and functional design requirements may conflict with the safety requirements. The safety analyses must show any conflict and provide enough detail to enable corrective action to be taken.

System safety has been critized for a great proliferation of analyses. As many as thirty-five different analyses have been listed. Some effort has been expended in attempts to standardize on several specified analyses with little success. Standardization of an analysis method is not the proper approach at this time. Specification of an output resulting from a credible analysis is appropriate. Some outputs of system safety analyses are shown on Figure 10. The main inputs supplied to the systems engineering process are the safety requirements that must be imposed on the system to make it safe enough.

The system description, functional flows and time line analyses provide the basis for the system safety analyst to identify the hazardous elements and conditions inherent in the system. The information may be analyzed, using a tabular format such as the Preliminary Hazard Analysis or the logic network format of the fault tree analysis. If the output required is qualitative, which is usually the case in early program phases, the time line data, functional flows and hardware descriptions are adequate. If a complete risk evaluation is to be made and a numerical requirement for safety is imposed in the system, more definitive design data is required. This information often is provided by reliability specialists. The failure mode and effect analysis contains most of the information needed. Care must be taken to consider the Failure Modes and Effects Analysis (FMEA) results from a safety viewpoint which can have a different criticality than the effect on reliability.

Hazard Identification

Experience retention, in the form of data taken from previous programs and personal experience of qualified system safety personnel, provides the basis for the initial identification of hazardous elements and conditions. High energy levels, hazardous environments, toxic gases, and structural problems are some of the first considerations. The type of fuel to be used dictates the ignition proofing requirements that must be imposed. The use of explosives requires many well established requirements to be imposed.

The environment the system is intended to operate in dictates requirements for adequate oxygen, thermal protection, shock or acceleration limits, etc. Safety factors for pressure vessels and basic structures must be established with proper consideration for the functional use of the equipment. For instance, the safety factors for pressure vessels on unmanned systems can be much less than for manned systems. However, care must be taken to be sure that such tanks are not pressurized when personnel are maintaining

the system or checking it out for launch. The identification of hazards continues throughout the entire safety program. As more is learned about the system, additional hazards become apparent. All hazardous elements and conditions should be recorded and action taken to control them to prevent accidents.

Hazard Potential Effect

The emphasis given to the control of hazardous elements is dependent on the potential effect or accident that could occur if control of the hazardous element is lost. This part of the analysis looks at all possible ways an accident could occur. The probability of the event occurring will be considered later. There are two ways this part of the analysis may be conducted. The analysis may start at the part level and continue through the subsystem and consider the system as a whole. The analysis can also start as a top down analysis, such as the fault tree analysis, which starts with an undesired event, and then goes down through all series of events that could occur to yield the undesired event. Single thread failure analyses are helpful but multiple failures must be considered to make the analyses complete. A fuel leak may increase the hazard level but a catastrophic event may not occur without an ignition source. In the case of hypergolic fuels, two leaks may be necessary.

The potential effect may be categorized as catastrophic, critical, marginal, or negligible as is required by MIL-STD-882 and NASA NHB 1700.1. This grouping enables increased emphasis to be given to the worst category. However, all of the hazards and their potential effect should be listed and provided to systems engineering. This data is essential and must be considered during trade-off studies. Also, each of the items listed should be closed out to show what preventive actions have been taken to prevent an accident from occurring. The hazard analysis format established in D2-113072-1, (8) "System Safety Analytical Technology - Preliminary Hazard Analysis," provides for the tabulation and recording of the identification of the hazard, subsystems involved, the potential effect, the category, and the recommended preventive measure to control the hazard.

Probability of Occurrence

The amount of resources that will be applied in preventive measures depends not only on the potential effect, but also on its probability of occurrence. An excellent example of this is the potential of meteorite damage to spacecraft. The effect of a meteorite hit would be catastrophic. However, the probability of significant hits is so small that resources have been diverted from meteorite protection to more effective areas in the spacecraft.

There are two methods of determining the probability of occurrence of accidents. The qualitative approach such as probable, possible or improbable can be used. This approach is very subjective and must be based on empirical data, experience retention or just plain engineering judgment. It is used on most safety programs today. The quantitative approach uses the best failure and statistical data to determine more accurate probabilities of an event occurring. A method of using FMEA data in a Fault Hazard Analysis provides some degree of quantification. The most thorough method is the Fault Tree Analysis which is used on weapons systems such as Minuteman and the Short Range Attack Missile (SRAM) where the undesired event is so serious that a numerical limit is imposed by the customer. The Fault Tree Analyses may be used for either qualitative or quanitative analyses. It has been described in numerous papers (9, 10, 11) and is documented in D2-113072-2, (12) "System Safety Analytical Technology - Fault Tree Analysis."

Corrective Action

The output of system safety analyses is shown on Figure 10. Each of them are of importance to systems engineering. Some of them such as inputs to trade studies and critical systems lists can be used directly. The safety requirements that result from the analysis will be covered later. The systems

engineering approach provides the way for the system safety input to be integrated into the mainstream engineering effort and to cause the implementation of the corrective action that is necessary to assure a safe system.

Safety Requirements (See Figure 11)

The systems engineering process defines the system and then establishes the requirements for what must be included in the system design and operation. The system safety requirements initiated from experience retention data are upgraded as more information is obtained from the above analyses. As mentioned earlier, they also include appropriate standards and guidelines developed for other programs. When combined into a single document they are readily available to all levels of the contractor and customer organizations. The requirements document should be divided into design requirements and operational requirements. Design requirements include the systems requirements and more specific requirements for each of the subsystems components and parts. Operating requirements specify what must be included in procedures to enable the as-designed system to operate safely.

System Safety Assurance (See Figure 12)

System safety assurance is used by this writer to include all of the safety effort expended to assure that the design and operating safety requirements are included in the system and that they are adequate. Figure 12 lists the activities involved. The systems engineering process control of the technical program includes reviews, trade studies, change control, and audits. System safety must participate in these activities to assure that safety is included in the design and operation of the system.

Program and Design Reviews

The entire series of program and design reviews provide an excellent opportunity for system safety to follow-up on the safety program. The system safety design requirements document provides an excellent baseline for safety review. The design can easily be reviewed against the requirements and extra emphasis can be given to looking for weak points in the safety program. System safety sign-off should be required at all such reviews.

Drawing Reviews

System safety requirements should indicate which drawings require safety review and sign-off. In some programs all drawings must be signed off by safety. In less hazardous programs only those items that are termed critical to safety receive such sign-off. Again the control inherent in the systems engineering process provide the means for system safety to carry out its function.

Configuration Control

It is not enough to prove that the initial design is safe. As stated earlier, all subfunctions of systems engineering must be aware of all changes to the system. This is especially true of system safety. Some of the worst accidents in past programs have been caused by lack of safety considerations of changes to the system. This includes changes to operating procedures as well as design changes. System safety should have the same sign-off responsibility on changes as it does on design reviews. Here again the systems engineering change control provides the means for system safety to "work within the system" to carry out its functional responsibilities.

SUMMARY

The primary purpose of systems engineering is to assure the optimum allocation of resources to achieve mission objectives. Consequently, the entire system safety program is aimed at achieving the safest system possible within program constraints and to further assure that this safety level is adequate. A decision of a program manager that a system is safe enough is a difficult one at best. To

the extent that the system safety program can contribute toward that decision with meaningful data, effective program controls and credible measurements of results, system safety activities will be able to demonstrate their value and successfully compete for the limited resources that any program has.

REFERENCES

(1) AFSCM 375 series, "Air Force Systems Command Manual - Systems Management, "June 1964.

(2) MIL-STD-499 (USAF), "Military Standard - System Engineering Standard."

(3) MIL-STD-882, "Military Standard - System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for."

(4) NASA Office of Manned Space Flight Safety Program Directive 1-A, "Safety Requirements for Manned Space Flight."

(5) NASA Safety Manual NHB 1700.1 (V-3), "System Safety," 6 March 1970.

(6) Grose, Vernon L., "System Safety in Rapid Rail Transit," Presented to the Rail Transit Conference, San Francisco, California, 13-16 April 1971, p. 2.

(7) Air Force Systems Command Handbook DH 1-6, "System Safety."

(8) Boeing Document D2-113072-1, "System Safety Analytical Technology - Preliminary Hazard Analysis." (Available from the the Defense Documentation Center.)

(9) Mearns, A. B., "Fault Tree Analysis, the Study of Unlikely Events in Complex Systems," System Safety Symposium, Seattle, Washington, 8-9 June 1965.

(10) Feutz, R. J. and Waldeck, T. A., "The Application of Fault Tree Analysis to Dynamic Systems, "System Safety Symposium, Seattle, Washington, 8-9 June 1965.

(11) Crosetti, P. A. and Bruce, R. A., "Commercial Application of Fault Tree Analysis, "Ninth Annual Reliability and Maintainability Conference, Detroit, Michigan, 20-22 July 1970.

(12) Boeing Document D2-113072-2, "System Safety Analytical Technology - Fault Tree Analysis." (Available from the Defense Documentation Center.)

SYSTEMS ENGINEERING

MISSION AND REQUIREMENTS ANALYSIS
FUNCTIONAL ANALYSIS
EXPERIENCE RETENTION
TRADE STUDIES
REQUIREMENTS ALLOCATION
DESIGN/OPTIMIZATION EFFECTIVENESS ANALYSIS
SYNTHESIS
TECHNICAL INTERFACE COMPATIBILITY
CHANGE AND CONFIGURATION CONTROL
DESIGN REVIEWS
ENGINEERING INTEGRATION
TEST INTEGRATION
PROGRAM REVIEWS
REPORTS AND EXPERIENCE RETENTION

FIGURE 1

SYSTEM SAFETY DEFINED

"THE OPTIMUM DEGREE OF HAZARD ELIMINATION AND/OR CONTROL WITHIN THE CONSTRAINTS OF OPERATIONAL EFFECTIVENESS, TIME AND COST, ATTAINED THROUGH THE SPECIFIC APPLICATION OF MANAGEMENT, SCIENTIFIC AND ENGINEERING PRINCIPLES THROUGHOUT ALL PHASES OF A SYSTEM LIFE CYCLE."

FIGURE 2

SIMPLIFIED SYSTEM SAFETY FLOW DIAGRAM

FIGURE 3

ESTABLISH SYSTEM BASELINE AND SAFETY GUIDELINES

FROM:

- o CUSTOMER REQUIREMENTS
  - o STATEMENT OF WORK
- o EXISTING GUIDELINES AND STANDARDS
  - o DH 1-6
  - o SFCM 8080
  - o FED CODES
- o EXPERIENCE RETENTION INFORMATION

FIGURE 4

IDENTIFY HAZARDOUS ELEMENTS AND HAZARDOUS CONDITIONS

- o PRELIMINARY HAZARD ANALYSIS
- o FAULT HAZARD ANALYSIS
- o FAULT TREE ANALYSIS
- o OPERATIONS HAZARD ANALYSIS

FOR

COMPONENTS
SUBSYSTEMS
SYSTEMS
INTERFACES
OPERATIONS

FIGURE 5

DETERMINE RISK INVOLVED

- o QUALITATIVE
  - o CATASTROPHIC
  - o CRITICAL
  - o MARGINAL
  - o NEGLIGIBLE
- o QUANTITATIVE
  - o STATISTICAL PROBABILITY
  - o PASSENGER MILES/FATALITY
  - o FATALITIES PER YEAR
- o COMPARE WITH COST AND DEGRADATION OF FUNCTION

FIGURE 6

ESTABLISH PREVENTIVE MEASURES

SAFETY REQUIREMENTS AND CRITERIA
- o DESIGN
- o OPERATIONAL
- o PERSONNEL

ORDER OF PRECEDENCE
- o SAFETY DEVICES
- o WARNING DEVICES
- o SPECIAL PROCEDURES

INTEGRATE WITH SYSTEMS ENGINEERING

FIGURE 7

SAFETY ASSURANCE (FOLLOW-UP)

- o DRAWING REVIEWS
- o DESIGN REVIEWS
- o FIRST ARTICLE INSPECTION
- o PROCEDURE REVIEWS
- o TESTING
- o LIAISON AND SURVEILLANCE
- o AUDITS

FIGURE 8

ESTABLISH AND MAINTAIN REQUIREMENTS AND STANDARDS (UTILIZING SAFETY ANALYSES)

INPUT REQUIRED

- PROGRAM REQUIREMENTS
- FUNCTIONAL REQUIREMENTS
- OPERATIONAL REQUIREMENTS
- EXPECTED ENVIRONMENTAL CONDITIONS
- EXISTING STANDARDS
- OTHER SUBFUNCTIONS RQMTS.
  - RELIABILITY
  - MAINTAINABILITY
  - HUMAN FACTORS
- ALLOCATE REQUIREMENTS

OUTPUT

- SPECIFIC SAFETY RQMTS. & STDS.
- INPUTS TO:
  - DESIGN & PROCEDURES
  - SAFETY DEVICES
  - WARNING DEVICES
  - TRAINING
  - PERSONNEL
- REQUIREMENTS FOR FURTHER ANALYSES, TRADE STUDIES & TESTING
- BASELINE FOR PROGRAM REVIEWS & AUDITS

FIGURE 11

ASSEMBLE BACKGROUND AND EXPERIENCE RETENTION INFORMATION

INPUT REQUIRED

- SYSTEM DESCRIPTION
- EXPER. RETENTION INFO.
- INFO. FROM SIMILAR CURRENT SYSTEMS
- HISTORICAL ENVIRONMENTAL DATA
- SUBFUNCTIONS EXPERIENCE RETENTION DATA
- RESEARCH

OUTPUT

- INITIAL SYSTEM SAFETY STDS.
- EXPERIENCE DATA FOR
  - QUALITATIVE ANALYSES
  - QUANTITATIVE ANALYSES

FIGURE 9

SAFETY ASSURANCE ACTIVITIES

- DESIGN REVIEWS
- TRADE STUDIES
- CHANGE CONTROL
- TEST
- DOCUMENTATION
- TRAINING
- PROGRAM CLOSEOUT

INPUT REQUIRED

- DESIGN CONFIGURATION
- TRADE CANDIDATES
- DESIGN CHANGE CONFIGURATION
- HISTORICAL

OUTPUT

- SAFETY ASSURANCE
- SAFETY OPTIMIZATION
- EXPER. RETENTION DATA
- INTEGRATED SAFETY PROGRAM

FIGURE 12

ANALYSES

- QUALITATIVE
- QUANTITATIVE

INPUT REQUIRED

- CURRENT SYSTEM DESCRIPTION
- FUNCTIONAL FLOWS
- TIME LINE ANALYSIS
- MISSION OBJECTIVES
- MISSION GOALS
- KEY MILESTONES
- REQMTS. OF OTHER SUBFUNCTIONS
  - RELIABILITY
  - MAINTAINABILITY
  - HUMAN FACTORS
  - QUALITY CONTROL
  - LOGISTICS
  - DESIGN
- SYSTEMS ENG. RQMTS.

OUTPUT

- IDENTIFY HAZARDOUS ELEMENTS & HAZARDOUS CONDITIONS
- IDENTIFY RISK
- INPUTS TO TRADE-STUDIES
- CRITICAL SYSTEM LIST
- CRITICAL OP. LIST
- CHANGE RECOMMENDATION
  - DESIGN
  - PROCEDURE
- SAFETY PREDICTIONS
- ALLOCATIONS
- INPUT TO SAFETY RQMTS.

FIGURE 10

SESSION IV

QUESTIONS AND ANSWERS

JERRY LEDERER: I don't have a question, I have an observation. That is in connection with Mr. Packard's statement that he wants to withdraw all the disciplines of safety and put them back into basic engineering. I have another document of his which requires that a hazard analysis shall be made on hardware, and I don't see how he can reconcile the two points of view. I am using that last document within NASA to promote further interest in system safety.

DR. BALL: Could I comment on that Chuck. I think this is an important point, consistent with what Mr. Lederer has been pushing himself for several years. The need for a risk analysis or even in the case of the Boeing Company, the Board of Directors requiring a risk-study report at the beginning of each program in which all the risks, risk of cost overrun, schedule slippage, the risks of failure to achieve a required technical characteristic like flight speed or safety reliability, this I think is very much in its ascendancy. Now of course Mr. Packard, I believe, and others are looking for the main stream program manager and chief engineer to submit these risk-study reports. You then have the safety engineer as one of the staff men helping the main stream. This is my overall point. The need for the services of the system safety engineer are increasing but it is as a staff to the main stream action, not as an independent staff working independently of the main stream.

MR. MILLER: Yes, I would definitely like to comment on that. I don't know who of repute in the business has ever suggested that safety was other than what you just described. If such a situation was led to take place, I will point the finger at the management of the organizations who allowed this to happen.

QUESTION: My question is directed to Chuck Miller. Chuck, we have heard an awful lot today about MIL-STD 882 and the application of this to weapons systems, but would you care to forecast how this looks in the civil aviation business, the application of system safety, including light planes.

MR. MILLER: First of all I think like any safety program document, if you look around when you think about applying it, you'll find that its elements are already being applied. I think this is true if you think of 882 in a civil aviation environment. For example, the FAA in recent years has undertaken what they call a Systems Worthiness Analysis Program which is another term for a form of audit. Certainly, these things are going on in the entire system, not just the FAA. The SST Program had safety work in it. John can tell you that the 747 had quite a bit of effort along this line. On the other hand, there are things that are not being done. As a matter of fact, the Safety Board had addressed two of these things in the past year, if I recall, one was in connection with a commuter airliner problem in which there was a control system failure which was one of the Board's specific recommendations to the FAA to consider in an 882-type hazard analysis. A similar recommendation the Board made involved the FAA's ATC system, their traffic control system. We looked, and this happened to be a general aviation case out in your area, Jack, where a controller misidentified or I should say failed to identify a certain target on his radar scope and proceeded to have his aircraft fly into a mountain as a result. Our question was, and it turned out to be a recommendation, why don't you apply hazard analysis techniques to the man/machine environment situation existing in an ATC Center. In other words, these are highly analogous to problems that NASA faces when they are looking at say a launch problem. I will say this though, I think the incorporation of something like 882 in civil aviation would be an even tougher job than it is in DoD for this reason, you have a very elusive buyer-seller-regulator relationship. Especially when you go across the full spectrum of aircraft from say an air carrier, which is relatively highly

regulated, to a general aviation operation which is in a relatively low regulatory status. So I am saying, it is a tough job. The thing that is missing to me is that when I look at civil aviation and compare it with the DoD approach to system safety, I don't see a system safety program plan. I don't know who you go to in a civil aviation business and honestly ask a question about a new aircraft being introduced or a major modification being made, who really has this thing laid out in total program planning fashion. Right now I think the answer is no one. I would submit that this is the first step. I think we will evolve into it whether it is called MIL-STD-882, FAR, or whatever it is, but yes I think these principles are going to rub off, I think they already have and I expect to see more of it.

MR. MCGUIRE: Chuck, I have a question along that line. Wouldn't you think some of the seller-buyer relationships that Dr. Ball discussed might figure in civil aviation, commercial particularly.

CHUCK MCGUIRE: Definitely, as a matter of fact, two years ago there were some rather interesting discussions at the top levels of the Air Transport Association about the possibility of them instituting the MIL-STD-38-130A in some modified fashion for industry, that is, between the airline/industry operators and manufacturers. I never have fully understood why this suddenly came to a halt but at least it was explored at that time, about two years ago.

GEORGE CRANSTON: I have a comment and then a question. I think we have had two very fine sessions and I want to express my appreciation to the speakers and to the Chairman for this personally. I think probably we would all like to do that. I suggest we give them a hand. Second, I think one of the most significant things we have heard in this conference was brought out this morning, the fact that we need or I have felt we need more work, specific work done by individuals on developing specifications that Chuck and Dr. Ball brought out, and implementing our standards and our general guidelines that we have now. I think we have let up on this and are resting on the laurels of trying to go with the standard. A lot more work needs to be done at this time on manuals and specifications at all levels in our organization and I wonder what you think.

DR. BALL: I'd like to express a similar thought but change the emphasis a little towards check list. For example, after the Apollo 13 experience which I think was a magnificent tribute to pre-planning and pre-analysis in that it allowed corrective action to take place, there were lessons to be learned there. The question is now, show me how the lessons learned have been fed back. Now you can say, well, we changed this paragraph of this policy or this paragraph of this specification but I think we need the check list as the connecting link. We should show the check list items for liquid oxygen tanks; the check list items for configuration management, because there were some problems there. Those check lists can then get fed into the University teaching courses we heard about this morning, they can get fed into the next revisions of our policies and specifications. But, because it takes so long to negotiate in our democratic way to get a spec out, I think we've got to do a much better job of formal conversion of experience in the check list form.

CHUCK MCGUIRE: You are leading into my favorite subject and you and I both are aware of the effort now going on in Skylab to come up with a check list similar to the one you have described.

JACK FRENCH: I would like to say that at MSC for each mission safety has to stand up and be counted as to whether we feel there are acceptable or unacceptable risks, etc. We stand up along with other directorates such as Flight Crew Operations, Flight Operations Directorate and various engineering and program offices. This requires a backup of a knowledgeable assessment group to assess the engineering and operations aspects throughout the "life-cycle" of the operation. You can't just rely on the design engineers to give you this. You need an independent group of very knowledgeable people who have as much knowledge about a system design as the system designers themselves. I just want to bring this out, that I feel that we do need an independent group. At MSC we do have a group of people, they are support contractors who

support us in this effort. I might add that at MSC also within the safety group is the continuity of experience from Mercury to Gemini to Apollo and Skylab that you don't have in too many departments.

MILTON: I submit one to Dr. Ball. One of the problems I think that we are going to have to face is that we can't afford to have anything less than absolute maximum safety in any program we've got. Just as you mentioned, now NASA is so loaded with good experienced data with problems faced, conquered, and now put completely to bed hopefully that will not arise on something like the Space Shuttle. Do you think we can afford anything less than having all the possible data to give to each contractor and then do a safety evaluation merely on the organization and the experience rather than in the approach to it. Again, as you pointed out on the chart, sometimes safety people are only talking to safety but as we have experienced in both DoD and NASA programs, safety usually doesn't count a single solitary point when it comes to selection of a contractor. I don't think simply having a safety plan in there someplace that it is recognized because everything else is tied to the speed capability, the altitude capability and all of these other performance items. Therefore safety usually only comes into being when you are finally in a negotiation and actually implementing the program and yet it has, as I say, zero weight in the selection of a contractor. Therefore, by giving every contractor as much of this data as you have available, even though it is all the same, you are not really putting one in contention against another.

DR. BALL: I think that is a very fine question. Let me be clear that my answer is personal and doesn't represent a NASA position. The answer is in two steps. During the contractor selection process I personally favor asking the contractor, what are you going to do to assure safety? If he tells me for instance, he has had the initiative to go to MSC where Jack French and Marty Raines have got some very fine documents such as safety hazard catalogs, and he has taken those catalogs from MSC; he has picked up other things from Irv Pinkel at LeRC and integrated these into his design decision process, processed them and provided them to our mechanical designers, etc., this is the opportunity for the contractor to tell us, during the competitive period. Once you have selected a contractor, then I think we should pull out all the stops in telling him everything we know. I think we should say, now look, lets sit down together and go over the total available knowledge and the sources of information that are available. The contractor may or may not pick that up and use it and through the award fee, then I want to trace the usage of funds. For instance, if I can get ½ or 1 % for safety out of a 15% fee I want to be able to check on the use of those resources. Is it evident the contractor's design decisions really are tapping all this knowledge? I think the appeal you made, don't hold back anything you know, I agree with, but the time I wish to feed that in is after contract award.

CHUCK OVERBEY, KSC: I'd like to amplify one point made by Mr. Miller and that has to do with the commercial aviation field. First, those of us who have worked with military missiles and in the case of NASA with the vehicles and spacecraft, a lot of us feel that we have had a free ride and in many ways we have, from a safety viewpoint. We have been the designers, we have been the buyers, and we have been the operators. As such we have been able to specify safety measures from one end to the other. When you get into the commercial field, in particular general aviation, that is a different world. I was with the CAA for about 10½ years and you just don't dictate beyond a certain point. A light airplane in particular is a consumer product and it is a different situation entirely. Take the Bonanza, a light airplane built by Beech, it costs about $100 for a 100 hour inspection. Everytime you fly the airplane for one hour you have to devote a dollar to inspection. That is the minimum requirement for FAA. If you go on and on with requirements, you will find that pretty soon you no longer have a consumer product.

JERRY LEDERER: I would like to reinforce that. For three years I was in charge of all civil air regulations and we were dealing with a very difficult situation as Chuck has just mentioned. NASA and DoD are virtually autocracies; they can dictate. You can't

dictate in civil aviation. You can do so more with the public carriers involved like the airlines, but not where general aviation is concerned. I recall in 1940 we had a case of a man chartering an airplane in Williamsport to fly to Newark, getting caught in weather with a commercial pilot, and getting killed because he lost control of the airplane. I immediately instituted procedures to require all commercial pilots who offer themselves out for hire to have instrument ratings, and the hue and cry against that proposal was terrific. First of all we were told there were not enough instructors to give the necessary instruction and they felt it would be a drag on the industry. This dragged on for a long time and then the war started and saved me from further problems. This is the way it goes, it isn't like working for NASA or DoD when you get into civil aviation.

MR. BOLGER: I would like to add a postscript to that and something Hank back there commented on. You know, I think you made a statement that you don't win a program because of a safety effort but you can sure lose the follow-on without it. This same feeling pops up in the civil aviation field. I have found, and you might call it a threat if you want to, but I have seen airlines, small ones albeit, put out of business because of accident problems. I have seen some big ones get awfully concerned over potential accidents and take action which they might not otherwise have taken. I have heard Presidents of the General Aviation Manufacturers companies get up in meetings within the past year and do a 180° in terms of the basic philosophy towards safety. There was a time not too long ago when some of the light plane manufacturers would stand up and say, "We are safe, everything we do is for safety and besides, let's not bring it out in the open because that will hurt sales." I have since heard some very powerful people in that business stand up and say, "We know that we cannot survive as an industry without increased effort on safety."

What I am suggesting here is that there is an awareness of a more difficult problem, but there is also an increasing awareness, as I see it in civil aviation, on the consequences of failure in inadequate safety programs. This is litigation influence? I don't know! Is it the influence of the overall public concern for safety? I don't know, but it is there. General aviation people, manufacturers, operators are more acutely aware of the failures due to lack of a good safety program today than I think they ever were before.

JOHN GRISWOLD: This will be just another postscript to the comment from the back of the room. Just recalling within this year, 1971, and seeing the results of some debriefings, I know of two contract awards which the statement was made, somewhat like this, that the proposed safety program that was described in that proposal had a significant impact in the selection of the winning contractor. You can interpret significant impact anyway you want, but it is something bigger than zero as far as I am concerned.

SESSION V
SYSTEM SAFETY IN SPACE PROGRAMS

Session Chairman - Mr. W. J. Quinlivan

"The Viking Project Safety Program"	Mr. Donald H. Ward
"System Safety in the Operational Phase"	Mr. John Gera, Jr.
"Lunar Module Program System Safety"	Mr. William F. Scarborough
"System Safety in Manned vs Unmanned Programs"	Mr. George B. Mumma
"The Reduction of a 'Safety Catastrophic' Potential Hazard - A Case History"	Mr. Joseph P. Jones

THE VIKING PROJECT SAFETY PROGRAM

By

Mr. Donald H. Ward
Project Viking Safety Officer

NASA

Langley Research Center

Presented at the

NASA Government-Industry
System Safety Conference

At

Goddard Space Flight Center

May 26-28, 1971

INTRODUCTION

Before discussing project safety I would like to give you a brief description of the Viking Project, the Management assignments and the space flight hardware.

The Viking Project is part of a program for the exploration of Mars with the use of unmanned spacecraft. The objective of the mission is to significantly advance the knowledge of the planet Mars by direct measurements in the atmosphere and on the surface. Observations of the planet will be made during the approach and from orbit. Particular emphasis will be placed on obtaining information concerning biological, chemical, and environmental factors relevant to the existence of life on the planet at this time, at some time in the past, or the potentials for the development of life at a future date. Two spacecraft, each consisting of an orbiter and a sterilized lander capsule, will be launched separately by Titan/Centaur launch vehicles from Cape Kennedy during the 1975 Mars launch opportunity. The orbiters will be used to insert the landers into orbit about Mars. Scientific instruments on the orbiters will be used to obtain data to aid in the selection of landing sites. Each lander after separating from its respective orbiter will soft land on the surface of Mars and transmit scientific data back to earth for a minimum of 90 days.

PROJECT MANAGEMENT

The Office of Space Science and Applications, Office of Planetary Programs at NASA Headquarters is responsible for the Viking Program Management. The Langley Research Center, Viking Project Office, has responsibility for overall Viking Project management. The Project is divided into five major systems as shown on Figure 1. The Lewis Research Center is responsible for managing the Launch Vehicle System. Figure 2 shows the Viking Space Vehicle. The space vehicle is composed of the Titan III, the Centaur, the Orbiter, the Lander, and the nose fairing. LeRC, as Launch Vehicle Management Center, is responsible for providing the Titan, the Centaur, the nose fairing, and for space vehicle integration. Space Vehicle Launch Management has been assigned to the Kennedy Space Center.

The Jet Propulsion Laboratory is responsible for managing the Orbiter System, and the Tracking and Data System. Figure 3 shows the Viking Spacecraft. The lander is enclosed in a bioshield and is shown attached to the bottom of the orbiter in this figure. The spacecraft is attached to the launch vehicle in an inverted position from that which is shown. The Orbiter System is responsible for providing the orbiter and the adapters on both the lander side and the launch vehicle side.

The Tracking and Data System provides the ground based system of tracking stations and communications networks required to fly the spacecraft and receive data; however, there is no flight hardware provided by this system.

In addition to overall Project management the Viking Project Office at Langley has responsibility for managing the Lander System and the Launch and Flight Operations System. Figure 4 shows the Lander System flight hardware. The Lander System consists of the lander; an aerodecelerator system consisting of an aeroshell, a base cover, and a parachute; and a bioshield to protect the lander from biological contamination after sterilization. The Launch and Flight Operations System does not provide any flight hardware but does utilize hardware provided by the Orbiter and Lander Systems in performing its responsibility to conduct spacecraft launch and flight operations.

I should point out here that the position of Project Safety Officer is a staff function within the Viking Project Office and reports directly to the Project Manager.

THE PROJECT SAFETY PLAN

Next I would like to talk about the development of the Viking Project Safety Plan, how the requirement for such a plan was established, and what I feel the plan does for Project Management in emphasizing and controlling safety.

The safety program on an unmanned NASA spacecraft project begins with the signing of the Project Approval Document. This is the initial document which authorizes project go-ahead and assigns the system level management functions which were described to you earlier. In the Project Approval Document each System Manager is assigned the responsibility for

safety of his system. He is required to perform that function in accord with the requirements of the NASA Basic Policy on Safety and the NASA Safety Manual.

The next step in developing the safety program is to include the safety task in the Project Plan. This is the top management document for the Project and records the Project objectives and various management arrangements for the Project including safety. It is signed by each System Manager, the Center Director for each participating NASA Center, and appropriate NASA Headquarters management personnel. The Viking Project Plan places overall responsibility for Project Safety with the Project Manager, with each System Manager being responsible for safety of his system. The Project Plan also states that the Project Safety Officer is responsible for developing and implementing a Project Safety Plan. Implementation of that plan will be the method of controlling Project Safety.

The requirement for a Safety Plan having been established, the task now becomes one of producing a useful document. During the time that the Project Plan was in an early stage of development and it was known that a Safety Plan would be required, a work statement was being prepared for development of the Lander System and Project Integration. As part of the integration support to the Project Office the contractor was required to prepare a Project Safety Plan. Martin Marietta Corporation, Denver Division, was selected for this effort and did prepare, under the direction of the Viking Project Office, the Project Safety Plan.

During preparation of the Safety Plan two basic facts that were mentioned a few moments ago had to be considered. First, the safety responsibilities had already been assigned by the Project Approval Document and the Project Plan and, second, the basic safety requirements we were to meet were already in existence. These requirements are contained in the NASA Safety Manual, NHB 1700.1, Volume I; KSC - KMI 1710.1A; and the Range Safety Manual, AFETR 127-1. With these considerations in mind it was decided that the plan should not be directive in nature but, rather, should identify within a single document those requirements which each System Manager and the Viking Project Office must accomplish to ensure an integrated safety program.

If the Project Safety Plan does not establish requirements and is not directive in nature, what value does it have to the Project and the safety program? I feel there are several important functions that the Project Safety Plan accomplishes. These are shown on Figure 5.

First, preparation of the plan requires technical interchange between safety personnel of the various systems early in the program. Certainly a plan is not required to have such an interchange but it does provide a focal point for such discussions. Next, the plan identifies the detailed responsibilities for each System and the Project Office. The Project Approval Document and the Project Plan are general in nature whereas the Safety Plan shows the specific tasks to be performed in fulfilling the general responsibility. Third, the detailed safety requirements are consolidated in a single document. As I stated earlier, the requirements we must meet are in existence. They are, however, located in many documents and the Safety Plan is an excellent method of consolidating these requirements into a single document. Finally, and I feel this is the most important function of the plan, it provides a method for review of the total Safety Program by top level NASA safety management personnel. This review ensures those of us working safety at the Project level that our planning is in concert with basic NASA Safety Policy.

I have discussed up to this point why we have a Safety Plan on the Viking Project and the function it serves. Now I would like to discuss the contents of the Plan with emphasis on the system safety requirements. The Safety Plan is divided into three basic sections with the first being an introduction. The second section deals with organization and responsibilities. The Plan covers the responsibilities I have already discussed but in much more detail. The third section of the Plan gives the Viking Safety Program Requirements and I would like to discuss these in some detail.

VIKING SAFETY PROGRAM REQUIREMENTS

The two new major pieces of flight hardware to make a first space flight on Viking are the Lander and the Orbiter. Referring to Figure 6,

our first requirement is that a detailed safety plan be prepared for each of these systems. These lower level plans will show both the system safety and operational safety tasks to be performed. Also included will be sections on industrial safety, and personnel training and certification. Our next requirement is related to safety at the launch site. We have consolidated the requirements of the Kennedy Space Center and the Air Force Eastern Test Range into a single grouping which shows those documents and procedures which must be prepared by the Project and approved by appropriate launch site agencies prior to launch. Next there are requirements in the area of industrial safety and for each participant to prepare an accident incident reporting plan. These two items are reasonably standard safety requirements so I won't go into details on them.

The Viking Lander will receive electrical power from two on-board Radiosotope Thermoelectric Generators. Use of these devices requires approval of the National Aeronautics and Space Council and its decision is based on a Safety Analysis Report. This report is prepared by the Atomic Energy Commission and is based on data packages prepared by the Viking Project participants. The Project Safety Plan includes a section on the requirements for these data packages and the responsibilities for preparing them.

Another requirement we have is for a Launch Readiness Review report on the status of safety. I would like to delay discussion on this until later because it is related to some points I want to make on how the project will monitor and control safety.

Last, but certainly not least in the order of importance, are the requirements in the area of system safety. The purpose of system safety is to avoid injury to personnel and to avoid any loss or damage to property. To accomplish this our first requirement is to identify all potential hazards and to eliminate them where possible. When elimination is not possible we want to reduce the hazard within practical limits. We then want to keep all levels of management aware of these residual hazards so that they may assess the risk involved in proceeding with the launch.

Potential hazards will be identified through analyses to be made of both the hardware design and proposed operations. After they have been identified each potential hazard will be categorized according to the risk associated with the hazard. A hazard reduction precedence sequence is established in the Safety Plan and will be applied to each hazard which is identified through the analyses or through any of the routine project reviews. The first item in the sequence is to design for minimum hazard. If a hazard is identified and can be reduced by a design change, such a change will be requested. When a hazard cannot be reduced through a design change, a safety device shall be incorporated into the system. Where it is not possible to preclude the existence or occurrence of a known hazard, warning devices shall be used to permit early detection of the hazardous condition. Finally, special procedures shall be used to reduce the magnitude of a hazard where it is not possible to eliminate it. Data on those hazards which are in a category that could result in death or disabling injuries to personnel, irreparable damage to the space vehicle, or damage to any ground equipment causing more than a 24 hour delay in the launch will be placed in the Viking Project Hazard Catalog.

Hazard catalog inputs will be provided by each system and the catalog will be maintained by the integrating contractor for the Project Office. First inputs will be made at or near each system preliminary design review and will be maintained thereafter until launch. This catalog will be the method by which Project Management is provided a record of the status of each hazard so that the proper assessment of the hazard can be made and appropriate management action taken when required.

MANAGEMENT REVIEW

The responsibilities have been assigned in detail and the requirements to be met by the Project have been identified. It is now the responsiblity of each system manager to implement those requirements within his system. As part of the overall management responsibility the Project Manager and his staff will review and monitor the safety effort being accomplished by the system managers. To perform this function the project has established a series of incremental reviews for each system culminating in a final Launch Readine Review two weeks prior to the first lau

These reviews cover all aspects of each system including safety. Inclusion of the safety effort in these project reviews is considered an important part of the Viking safety program. This action brings to the attention of project management those items which are being worked by safety personnel, it allows an open discussion of these items by a review panel with expertise in many technical areas, and it permits a method of tracking safety items to determine that a proper resolution of the item has been made.

CONCLUDING REMARKS

In conclusion I would like to say that it was not necessary to sell the importance of a good safety program to Viking Management. Safety has been an important element of the Project since its inception. A very good safety plan has been developed; however, at this point in time the flight hardware is still in design and the effectiveness of our safety program is unknown. Our goal is no accidents or incidents and two successful landings on Mars in 1976.

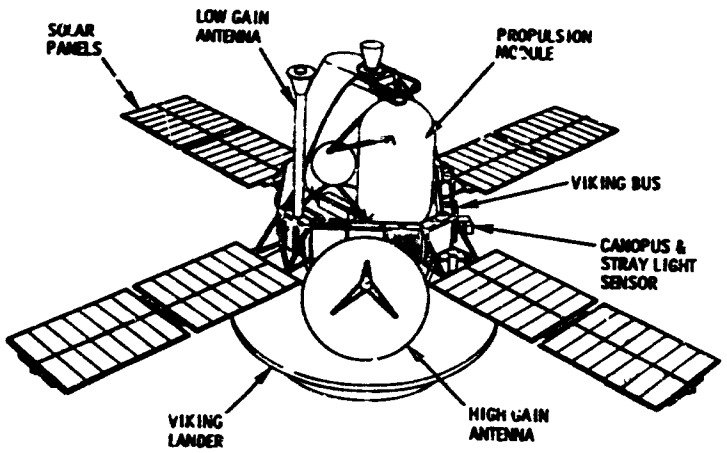
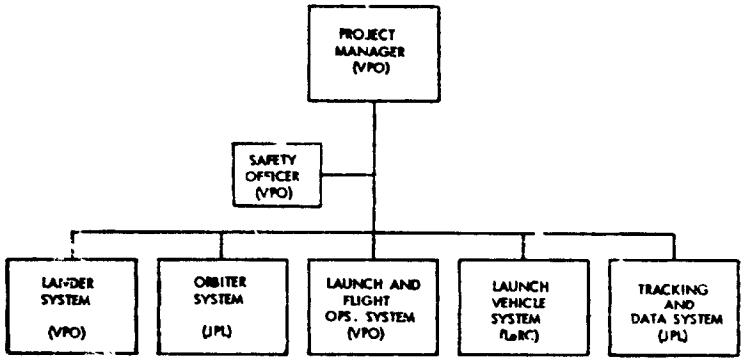


FIGURE 3 - VIKING SPACECRAFT



VIKING PROJECT MANAGEMENT

FIGURE 1

168

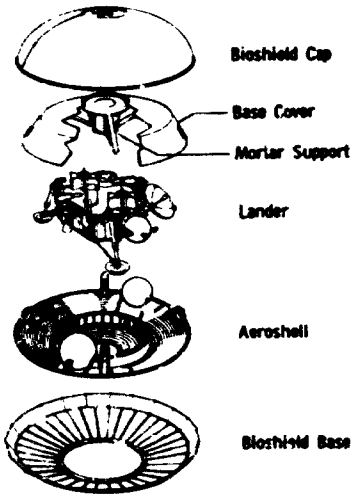


FIGURE 4 - VIKING LANDER CAPSULE

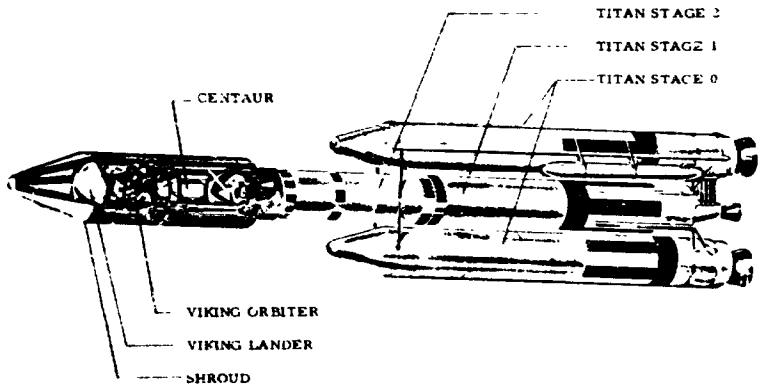


FIGURE 2 - VIKING SPACE VEHICLE

1. Requires technical interchange between project safety participants early in the program

2. Identifies detailed responsibilities for each system and the Project Office

3. Consolidates and identifies in detail the safety requirements in a single document

4. Provides method for top level NASA safety review

FIGURE 5 - FUNCTIONS OF THE SAFETY PLAN

1. Preparation of detailed Orbiter and Lander System level Safety Plans
2. Kennedy Space Center/Air Force Eastern Test Range Safety Requirements
3. Industrial Safety
4. Accident/incident reporting plan
5. Safety Analysis Report Data Packages
6. Launch Readiness Review Report
7. System Safety Requirements
   (a) Identify potential hazards through analysis
   (b) Eliminate or minimize hazards through a Hazard Reduction Precedence Sequence
   (c) Document Hazards in Hazard Catalog

FIGURE 6 - VIKING SAFETY PROGRAM REQUIREMENTS

N72-25977

SYSTEM SAFETY IN THE OPERATIONAL PHASE

By

Mr. John Gera, Jr.
Manager, Division Safety
North American Rockwell

PRECEDING PAGE BLANK NOT FILMED

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

SYSTEM SAFETY APPLICATION IN THE OPERATIONAL PHASE

The operational phase of a program assures completion of flight test programs and demonstration of operational capability. It is mission performance. Support of this activity from a System Safety standpoint is failure analyses, hardware changes, procedural changes, accident/incident analyses, and a great amount of involvement in ground operations. However, the operational phase really starts further back than at mission performance. I say this because one never finishes designing and manufacturing the system since requirements seem to change calling for improvements in the system. In this respect I consider the manufacturing, testing and material handling an important element of the operational phase and should be treated as such.

No one disagrees with the concept that a good, safe product starts with the designer. System Safety effectiveness also starts there. During its short life, the major emphasis of System Safety has been in engineering and we can find voluminous material on System Safety engineering management, System Safety engineering, System Safety analysis, and so forth. With the emphasis on engineering, we sometimes forget that System Safety is a totally encompassing task, as the word system implies. As a result, important processes in the total system go unattended. What good does it do to engineer a functional, safe product; build it on time within budgeted cost; then have it damaged by inattentive handling or worse yet by not having handling equipment because the interface was not there. Someone forgot -- someone overlooked. We need to stop and evaluate the total System Safety process to assure we really are talking about a "system" oriented program.

I'll cover System Safety concern in manufacturing, test operations, material handling, and flight test and flight operational phases. The reason for including manufacturing, test operations, and material handling is that is an area that has lacked proper System Safety concern.

Most manufacturing people do not have the luxury of knowing why certain hardware is designed a certain way. The engineer can only reflect the design in drawings and specifications after the thinking process had culminated in an end concept. The manufacturer could easily envision the end product differently from a process standpoint and, gentlemen, this process analysis from a System Safety standpoint desperately needs to be accomplished early in the program.

We need to:

1. Look at facilities for emergency backup power, electrical protection against main power fluctuations, work platform locations, deluge systems, lighting, noise, accessability. The relationship of this equipment on the end product.
2. Develop requirements for support items such as work stands, hoisting, confined entry, emergency procedures, safety critical operations such as welding and pressure tests.
3. Conduct hazard analyses o. the manufacturing flow and develop disciplines to eliminate or reduce these hazards prior to the start of manufacturing operations.

We have learned the hard way tnat playing "catch up" is expensive and very hard on the nerves, I might add. Lack of analysis has been the culprit in many instances, leading toward destruction of space boosters, test articles and components. Lack of process control has led to untold embarrassing situations. The accidents are often times shrugged off under the umbrellas of statements that "to err is human," "Murphy's law," and the like. It is often said, "We have time to do the job over, but never enough time to do the job right the first time." All of these so-called explanations are, in my opinion, unacceptable crutches and ways to avoid the basic problem. Many times we design traps for the men in manufacturing, test, and material handling. They need a good process analysis that can identify for them situations that are hazardous to the product as well as ways to protect them from personal injury. They need to be reminded about safety features required to assist them in doing the job right the first time.

Let's back up a little and ask ourselves why not let the builders and users work closely with the designer in the early stages of design. Not just involvement in the design review but during the criteria development phase and the

actual design. The outcome will be a safer and more efficient process along with being cost effective; the ground support equipment and handling equipment can be brought into the picture much earlier; and the transportation or movement of subassemblies and delicate parts can have parts protection considered during the design phase. You can already see that part of what we consider System Safety is getting everyone into the act not merely the system safety engineer but the people that are building, handling, and testing the product. System Safety, then, is part of the labor that goes into the product -- a direct labor function that is looked at very carefully as to its contribution. The payoff is accident prevention as opposed to cure.

(Refer to Chart)

Early analysis in the manufacturing process identifies not only what is required to build the product but also the required skills. Training and certification of personnel helps assure that the job starts correctly. The next step is to match the process against System Safety standards. Those of us who are fortunate in having active standards know many of the pitfalls in process delays are avoided by assuring standards are satisfied. If some standards cannot be satisfied, our job in System Safety is to work with respective departments and keep the process moving in a safe manner. This is our contribution that is looked at very carefully. Don't misunderstand me here -- I am not advocating disregard for standards by merely signing a waiver. What I am saying is that we in System Safety should not use the standard as a shield and say, "You can't do that!" The approach is -- "we have a problem!" and our job is to help get the program out of that problem.

Review of documentation comes next. These reviews require approval of safety critical systems. That is of systems that need tighter monitoring because of damage potential. Certain installations, pressure tests, major hardware moves at times require that extra pair of trained eyes from System Safety. So in these reviews we assure ourselves that planning documentation and process documentation have proper back-out procedures in case of problems; safety cautions and warnings are identified. Here again, we shouldn't only act as a filter -- we should be helpful in making constructive comments to make the process better and safer. Another word of caution -- the responsibility for safety must remain in each department with each supervisor and with each employee.

Testing operations provides a unique situation for System Safety. Testers must understand manufacturing since there always seems to be some finishing up to do after the hardware is manufactured. This discipline must understand handling techniques and adapt them to the hardware being handled while undergoing checkout. They must also understand launch checkout and launch procedures since testing attempts in every way possible to duplicate the launch conditions. The concept that is followed is manufacturers build and testers test, resulting in a better product.

Closing the loop is an element that many people overlook.

Along with the imposition of standards and reviews, a key element is monitoring, audits and surveys. This gives Safety the opportunity to evaluate whether or not operating departments are, in fact, living up to the safety standards. Modifications can be proposed through this performance monitoring, coupled with new methods, ideas, and worker behavior. We also have other sources; an important one being customer experience. Additionally, internal and external experience can be evaluated. The final element of the action or monitoring loop is feedback from the departments themselves in the form of communication monitoring and direct communication. When we combine all these elements of experience, performance monitoring, and communication, the next big step is to see if the resources we have available support the recommended changes and if these changes support the goals. We have to be practical here. System Safety has to consider the safety aspects but also cost effectiveness. Our talents are put to the test in walking the fine line between the two. An unbending, non-innovative, to-the-book System Safety department is worthless in this situation.

Our final step is to take the results of the analysis and feed them back in the form of constraints within the operating departments which can take the form of additional checks and balances in the control and procedural

documentation; in modifications to the system safety standards. I might add that these modifications can take the form of either being more stringent or in easing of requirements. This is a constant learning process. The other constraint is a feedback into the engineering world by way of requirements, specification changes, retest requirements, hardware protection, and the like.

In a short period of time, I have attempted to show a closed loop flow which includes the impact of good System Safety involvement in the early portions of the program as well as the very important feedback loop. It is obvious, if the involvement comes at some time after start of the program, we play "catch up" for the remainder of the program. You don't have enough trained safety personnel to go back and review every drawing that was pumped out, every drawing that is being pumped out now, and attempt to monitor and take action on the feedback loop. Gentlemen, you chase your tail and never catch it.

I indicated to you earlier that I consider manufacturing, test, and material handling a part of the operational phase. There are two elements of operations that fall within my definition of operational phase. The first has to do with manufacturing operations, test operations, and material handling operations. This is the potential damage from people, processes, procedures, checkouts, and the like. The second element is the hardware operation with potential damage to mission and crew from insufficient primary or secondary systems. In the latter, the safest possible approach for overcoming hardware operational problems or emergencies would be to develop all the equipment and procedures so that the crew would have the option to select the most applicable from the protocol of emergency actions. These emergencies could be single or combinations of explosion during boost or orbit; severe instability during boost or orbit; loss of thrust during boost; fire; trajectory deviation; capsule decompression; life support system failure; power failure; subsystems failure; and loss of retro thrust. And there are many more to consider in separation, docking, maneuvering and the like. However, recognizing the limitations in time, money, and manpower, there must be a reasonable investment in study analysis and development testing to determine what is practical. This activity provides a rationale for setting design requirements.

The several occurrences of failures in flight, both major and minor, serve notice, in view of space hazards and more ambitious programs, that added attention to the potential requirements for operational safety can be justified. These operational emergencies are serious incidents which interrupt, either temporarily or permanently, the normal course of the mission plan. As indicated, such incidents may be anticipated or may occur unexpectedly. Anticipated emergencies can be countered by careful planning and implementation of action prior to the event, redundancies, and rapid and efficient action following the event. These actions all fall under the category of analysis that takes place early, prior to the design phase. The unexpected emergencies are those that were not thought to exist or were overlooked. During the hardware operational phase, these are the ones that bother us the most. What did we forget. The number of possible operational problems is virtually endless. No situation or system can be seen that is entirely immune to all such events. We must select the credible accidents or emergencies and act on them. So from my introductory definition, I find it difficult to separate the "people building" from the "people operating" phase. Considerations must be there for both, early and continually. The actions taken early, prior to and during design phases, helps us get prepared to prevent emergencies and provide recovery actions. There is ample opportunity for Safety to become involved, to be able to raise questions as to readiness. The review process has matured and includes: the preliminary design review; the critical design review; the first article configuration inspection; flight readiness review; and the design certification reviews.

In summary, a continuing emphasis placed on preventing accidents or emergencies through hardware design, manufacturing, test operations, handling, and operational mission analysis can give us the greatest return possible in the area of safety for the resource expenditure devoted to that end.

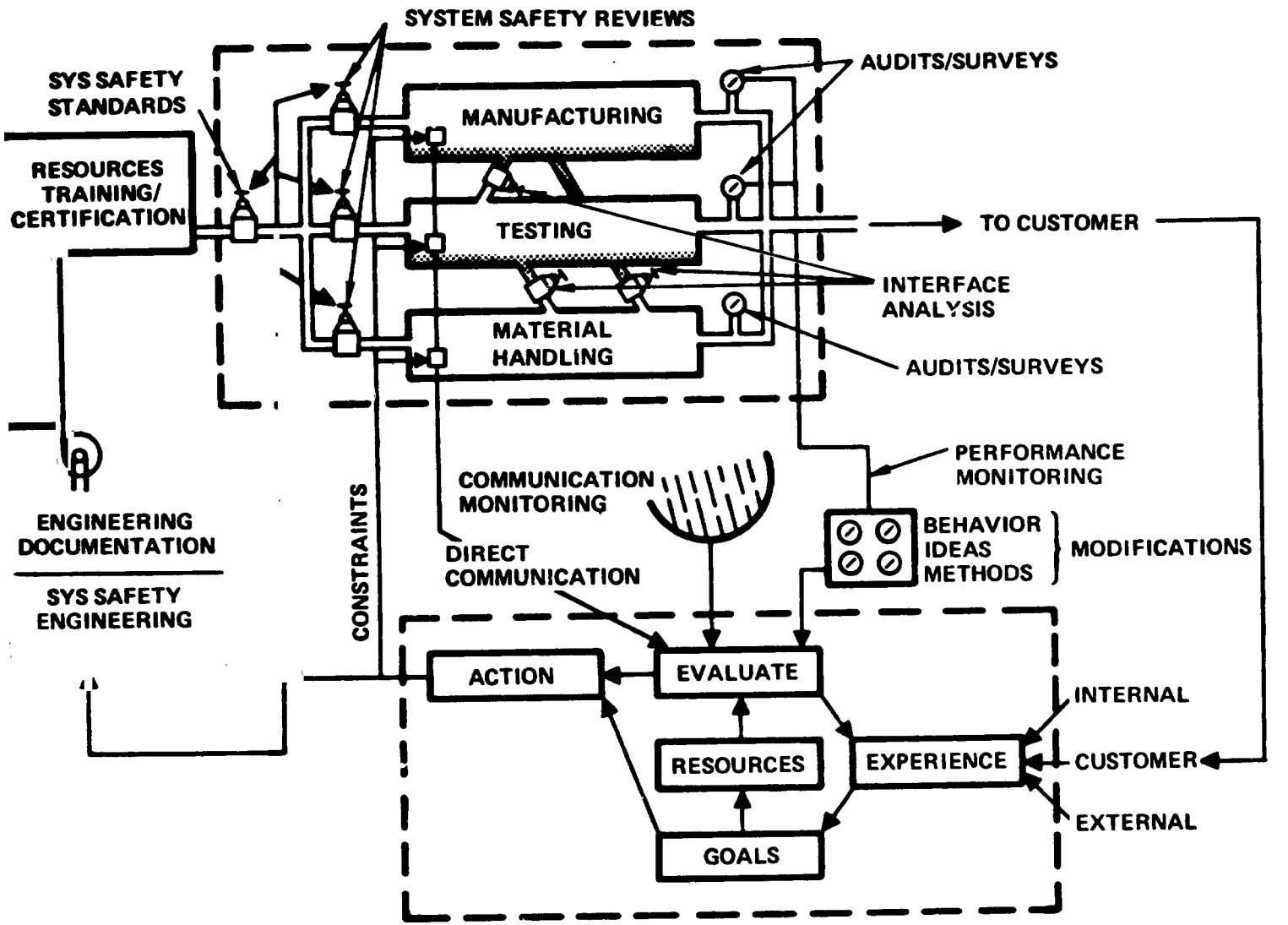

SYSTEM SAFETY REVIEWS
SYS SAFETY STANDARDS
RESOURCES TRAINING/ CERTIFICATION
MANUFACTURING
TESTING
MATERIAL HANDLING
AUDITS/SURVEYS
TO CUSTOMER
INTERFACE ANALYSIS
AUDITS/SURVEYS
PERFORMANCE MONITORING
COMMUNICATION MONITORING
BEHAVIOR IDEAS METHODS
MODIFICATIONS
ENGINEERING DOCUMENTATION
SYS SAFETY ENGINEERING
CONSTRAINTS
DIRECT COMMUNICATION
ACTION
EVALUATE
INTERNAL
RESOURCES
EXPERIENCE
CUSTOMER
EXTERNAL
GOALS

FIGURE 1

N72-25978

LUNAR MODULE PROGRAM SYSTEM SAFETY

by

Mr. William E. Scarborough
LM Safety Manager
Grumman Aerospace Engineering Corp.

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

During the development of the Apollo Program spacecraft, the complexity of the vehicle systems and the pressures of mounting costs and time schedules established a requirement for company and NASA management visibility to support intelligent decisions with respect to risk management. These considerations, with the added emphasis of the Command Module fire at Cape Kennedy in early 1967, led NASA to establish the Office of Manned Space Flight Safety and to implement formal safety programs at all NASA Centers and at major contractor facilities.

LM SAFETY

Gruman, as a major contractor, was authorized to establish a formal LM System Safety program covering the main production facility at Bethpage and field site operations at Houston, Cape Kennedy and White Sands. The Gruman safety effort prior to implementation of this LM System Safety program was limited to a test operations group working with the spacecraft assembly and test organization and an analytical safety effort within the LM engineering organization. This early effort, coordinated with Reliability and the engineering subsystems groups, had identified crew hazards in the spacecraft and had implemented hardware fixes or compensating operating procedures for the flight crew data file. The implementation of a formal program based on an approved System Safety Plan provided a consistent and systematic effort, increasing the probability of detection of potentially hazardous conditions by in-depth design review by the safety group.

OBJECTIVE AND SCOPE

The objective of the program was and is the elimination or reduction of risk to personnel, material, and facilities resulting from failures or malfunctions in hardware or procedures.

The scope of this wide-ranging program was an integrated engineering, test operations and industrial safety effort in direct support of LM design, production and test activity in the Bethpage area. Indirect support and liaison was provided to the Gruman field sites and NASA offices. Safety support included analysis of design and proposed design changes for flight hardware, ground support equipment and facilities; the exchange of information on hazard assessments and accident experience, and review and analysis of discrepencies and anomalies reported during ground test and flight operations.

REFERENCES

The NASA Safety Manual (NHB 1700.1) and the System Safety Requirements for Manned Space Flight (OMSF SPD NO 1A) are the primary NASA source documents for the LM System Safety Program.

Other documents utilized in the development and implementation of the Program include applicable Grumman Corporation Procedures and Federal, State and local statutory requirements, and the USAF Systems Command System Safety Design Handbook DH 1-6.

ORGANIZATION

The organizational structure adopted provided for a Manager on the staff of the LM Program Director heading a Safety group with two branches, System Safety and Test Operations Safety. The System Safety branch supports LM Engineering and provides liaison service to the field sites and to cognizant NASA offices. The Test Operations branch supports production and test operations and provides industrial safety service to all LM Program personnel and facilities.

LM Safety provides support on a day-to-day basis to all Program groups and, in turn, receives support from Engineering, Reliability, Q.C. and the Sub-Contract managers. This closely coordinated effort assures maximum utilization of all available documentation and avoids duplication.

SAFETY FUNCTIONS

There are four major functions of System Safety on the LM Program - Analysis, Review, Surveillance and Test/Mission Support. Each of the functions includes a number of detailed tasks - some basic to any system safety effort and some peculiar to the LM program.

• Analysis

The analysis function includes a hazard assessment of each spacecraft subsystem,

performed on a functional basis for each mission phase. The FMEAs (Failure Mode and Effect Analyses) from Reliability, the Mission Time Lines, and the documentation from other subsystem groups are utilized for a detailed study which considers both ground and flight crew operations as well as hardware failures in identifying hazards. The study effort classifies hazards as crew safety or mission success and confirms compensating provisions or backout procedures. Uncompensated hazards are reported to the cognizant engineering group and are tracked to final closeout by hardware or procedural changes.

This technique is also applied to proposed design changes, which are analyzed for personnel or hardware hazards and are followed-up through the approval cycle to installation and retest or rejection.

An example of the hazard assessment effort is the analysis which was completed for LM-5, the vehicle which flew on Apollo 11 and made the first lunar landing. The functional analysis of each subsystem was performed for the mission phases during which the spacecraft was active. The subsystem functions were evaluated for their effect on the flight crew, vehicle, and mission; the adequacy of contingency procedures, and other compensating provisions. The comparison of mission phase per sub-system function was related to methods of detection, time criticality, and availability of corrective or backout procedures. Uncompensated hazards were identified and evaluated and a rationale for their acceptance or rejection provided. This analysis revealed no crew safety hazards requiring hardware changes. All hazards identified were of the "acceptable risk" category based on the compensating provisions available in the vehicle. Procedural changes were recommended, however, to enhance mission success. These included an independent exercise of the redundant explosive device systems and constraints on attitude changes during the period while the lunar and command modules were "soft" docked on the capture latches. The capture latches are the devices on the Command Module probe which initially engage and lock-on to the LM drogue mounted in the top deck tunnel area. "Hard" docking is the subsequent action of retracting the probe and engaging the twelve docking latches.

This major analytical effort has since been utilized as a base-line study for the program, with each of the follow-up spacecraft reviewed emphasizing the hardware and mission changes incorporated since LM5. Analysis of these later vehicles missions has identified additional hazards which have been compensated by hardware changes or procedural workarounds incorporated in the crew check lists and mission rules.

- Review

The Review function includes those tasks involved on a continuing basis with the review of test and working documents and the operations they control.

Operational checkout Procedures (OCP) which are utilized for subsystem and system checkout are reviewed. Particular attention is devoted to revised procedures and to changes proposed during operations. The hardware setups utilized for tests are included, with emphasis on safety provisions such as relief valves, hose restraints, proper bonding and grounding and the like. Hazardous sequences in these operations are identified and marked and special control exercised while they are in-work. Real-time deviations to procedures are reviewed, with a safety concurrence and sign-off required for those designated hazardous.

An early and highly satisfactory Review effort was the Operational Readiness Inspection (ORI) conducted on the LM Internal Environment Simulator (IES). This altitude chamber facility was designed to provide checkout and verification of the LM life support system and involved manned runs in 100% oxygen environments. The ORI was conducted in accordance with NASA directive MSCI 8825.2, which establishes criteria for manned operations in oxygen-rich environments. GAC believes that the ORI conducted under 8825.2 is an extremely valuable safety tool for any facility requiring man-rating. Effective program cost control will tailor the ORI, the Board size, and the scope of activity to the hazardous nature of the facility being inspected.

Prior to the LTA-8 LM test vehicle operations in the MSC Houston altitude chamber, a review of the OCPs to be utilized during the tests was conducted by a special team of subsystem engineers, coordinated by LM System

Safety engineers. These tests, the first manned LM operations in a simulated space environment, were identified as extremely hazardous and a thorough analysis of every phase of the operation was conducted. The Safety Review team identified numerous procedural problems, all of which were corrected by changes to the documents prior to the chamber runs.

A similar review of the test documents to be utilized during the checkout of LM-1, the unmanned first flight spacecraft, was conducted at Cape Kennedy by the LM Hazard Review team. This review, chaired and coordinated by LM System Safety program personnel, covered thirty-seven documents and identified and documented fifty-three hazards. In three cases, hardware fixes were required and change requests were initiated. The remainder of the hazards were satisfied by procedural changes incorporated in the test documents.

For the first manned flight, LM-3 in earth orbit, the team reviewed the documents to be utilized for the preflight spacecraft checkout and altitude chamber runs at KSC. This team also identified more than fifty hazards requiring changes to the procedures, all of which were incorporated in the test documents. More important than these statistics, however, was the heightened interest stimulated in hardware, test set-up and procedural changes when the Safety Review was scheduled and imminent.

With each of these safety reviews, confidence in the spacecraft and the test procedures increased and on completion of the LM-3 assessment, formal reviews were terminated. However, procedural changes proposed during any test or operation are still reviewed and approved by Safety prior to their incorporation in the documents.

An additional Review task is the investigation and reporting of accidents which occur during production or test operations. On the LM Program, an accident is defined as any unplanned event which results in injury or damage to program material or facilities. All accidents are thoroughly investigated and reports submitted to cognizant management and NASA offices. Recommended corrective actions are tracked to close-out, with periodic status reports to responsible groups.

Experience on the Program to date shows a steadily declining accident rate, with 3.9 accidents per million manhours in 1969 and a low of 2.2 in 1970. During a one year period, from May '69 through May '70 more than 8,000,000 man hours were worked without a disabling injury. Analysis of the accident record indicates that the majority of the accidents are caused by carelessness and failure to follow procedures. Some typical examples include the following:

1. A facility technician installing a workstand on a concrete floor was setting studs with an explosive-actuated gun. To expedite the job, he attempted to drive a stud through a pre-drilled hole in a flange of the stand instead of using a clip held by an additional stud. Missing the hole, the stud ricochetted off the flange and floor and struck the man on the jaw, where it lodged and was subsequently removed surgically.
2. During installation of replacement components in the spacecraft heat transport (cooling) system a technique involving freezing the system fluid in the coolant lines with liquid nitrogen coils was being utilized. (This process permits cutting lines without draining the system or introducing air into the lines). An inadequate temperature gage and inattention by the man monitoring the temperature allowed the plug to thaw and pop out. Attempting to stop the flow of glycol, the technician held his thumb over the open line, suffering second degree cryogenic burns from the escaping fluid. In addition to the injury, extensive cleaning was required to remove the spilled glycol from wire bundles and spacecraft structure.
3. At the start of the transfer of approximately 2500 gallons of waste alcohol from a facility storage tank to a tank truck the 3" pickup hose ruptured, spraying approximately 100 gallons of alcohol over the truck and the surrounding area before the transfer pump was stopped. There were no injuries and no other damage although the incident was potentially catastrophic considering amount of alcohol involved and the ignition sources present in the area. Prompt action by the Safety Engineer and the Fire Guard covering the operation minimized

the spill and dissipated the free liquid. Cause of the accident was an unqualified driver-operator on the tanker who did not operate the pick-up pump and valves in proper sequence.

Also included in the Review function is the tracking of close-out action on safety-significant failures which occur during test or flight operations. While the primary responsibility for failure close-out action rests with the Reliability group, Safety is concerned with failures involving hazards to ground or flight crew personnel and makes full use of the Reliability documentation which is available. Identification of those failures for which Safety has a responsibility is based on criteria established by the Safety group in accordance with hazard classifications developed by NASA. Action in tracking these failures consists of coordinating with the responsible engineering subsystems groups and continuing the follow-up to final close-out.

LM Safety also reviews all ground support equipment failures, assessing hazards to personnel or hardware and coordinates with the GSE group on close-out action. For common-use GSE, which is shared with other contractors, an information exchange procedure has been established to assure timely corrective action on all hardware at all sites.

We have found that the daily Program Status meetings attended by the Program Director and Engineering subsystems managers, provides maximum visibility on developing problem areas and the opportunity to initiate immediate corrective action. This activity is a major day-to-day function of the system safety group.

- Surveillance

The surveillance function is primarily the activity of the Test Operations Safety group. All manufacturing and test facilities are monitored for compliance with safety requirements and for adherence to current Corporate Procedures and legal requirements of local and Federal safety statutes. Identified hazards are corrected immediately or the work area is tagged out-of-service. This coverage is provided by Safety on a full-time basis for all scheduled operations, 24 hours per day seven days per week.

- Test and Mission Support

Safety support of test operations includes participation in Test Readiness Reviews and Pre-test Briefings. Safety requirements and emergency procedures are reviewed with the test team and qualification of test team members confirmed with the Test Conductor.

Frequent surveys of test facilities are conducted to assure adherence to established safety requirements. Special attention is devoted to hoisting and lifting equipment, pressure hose restraints, proof testing of equipment, and installation of safeguards such as kick plates, guard rails, safety nets etc.

Test team training and certification (as required) are monitored and frequent drills in emergency shut down or back-out procedures are conducted. Authority for safety approval of deviations to hazardous test procedures is delegated to the safety engineer on duty. The Safety Manager is the only Authority for waivers - which are granted for one-time exceptions to established safety requirements or rules. In all such cases, additional specific safety requirements are imposed.

During hazardous test sequences or operations, a safety engineer is required to be present at the test site at all times. His support of the activity includes real-time approval of procedural deviations, equipment changes, and maintenance of a safety test environment throughout the facility.

For the Apollo Missions, LM System Safety engineers are assigned to the Mission Support Team and provide full coverage of all LM active mission phases in the Bethpage mission support room. Activity in this role includes participation in the mission simulation training runs, flight crew debriefings, and follow-up on flight anomalies and discrepencies.

SUBCONTRACT SAFETY

For the task of reviewing the safety of the Program sub-contractors, the LM Safety team monitors the formal review activity of the Reliability, Quality Assurance, and Sub-system Engineering groups which have primary responsibility. Reports are reviewed regularly and the safety group participates when required for on-site reviews. Documentation and advisory service are supplied to the regular inspection teams and to the resident personnel in

the plants. LM Safety provides personnel and participates on-call for investigations of accidents or when plant conditions involving safety are being reviewed. Recommendations resulting from investigations or reviews are made to Program Management, with follow-up to assure implementation of approved changes. This coordinated effort with QA group has been demonstrated to be a satisfactory, cost-effective method of monitoring a vast network of subcontractors.

FIELD SITE SUPPORT

An essential element of the LM safety effort is support of the Grumman field sites at MSC Houston and White Sands, with the Bethpage Program office providing policy direction and liaison between sites. The Houston operation is primarily manufacturing and test in support of Grumman activity at NASA.MSC. At White Sands, the company provides engineering and material support for the engine firing and propulsion system tests conducted in the test cells.

At KSC, the company maintains a safety group which provides all required functions for the local activity. Liaison and coordination for this group is also provided by the LM Safety organization at Bethpage, particularly in the area of spacecraft technical support and in the exchange of operational experience and information.

REPORTS

Management visibility, both for NASA and Gruman, is provided by regular and special reports of significant events and safety accomplishments on the Program. A monthly status report is provided to the MSC Safety office with other special reports as required.

An accident reporting system has been established to provide the background material for positive preventive action. All occurrences are recorded, utilizing a simple, one page form, and are followed-up until final close-out action is complete. Reports and periodic summaries are distributed to Program, Corporate, and NASA offices to assure maximum benefit to other groups with similar problems.

MEETINGS

Accident experience and preventive actions were also shared with other contractors and the NASA Centers by means of the STEMs (Safety Technical Exchange Meetings) sponsored by the NASA. These valuable meetings were scheduled periodically at the Centers or at Contractors' plants and provided a useful forum for the exchange of information.

Currently, the LM Safety group participates in regular Safety Concern meetings via telcons with the MSC Safety office. This coordinated approach avoids duplication and assures maximum effort on follow-up and close-out of identified hazards.

CONCLUSION

The application of System Safety principles to the LM Program has been eminently successful by any standard. In the face of the pressures of tight schedules and shrinking budgets, LM manufacturing and test operations have been on-time, with a continually declining accident rate. The LM spacecraft performance on the Apollo missions to date - from the first lunar landing by Armstrong and Aldrin in LM 5 to the latest by Shepard and Mitchell in LM 8 - has met or exceeded all mission objectives. The success of the total effort to put man on the moon marks Apollo as probably the most significant program of our age. As a small part of that total effort, LM Systems Safety made a contribution which will continue, maintaining or improving the standards established for the Program until the final Apollo mission is flown.

N72-25979

SYSTEM SAFETY IN MANNED VS UNMANNED PROGRAMS

By

Mr. George B. Mumma
Systems Safety Manager
Martin Marietta - Denver

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

In keeping with the theme of this year's conference, I would like to present to you the differences in applying system safety techniques to present space programs and highlight the role that system safety plays in providing management a working tool for determining the degree of risk or liabilities associated with both the manned and unmanned space programs. Two ongoing NASA programs will be used throughout this discussion for comparison; they are the Skylab Earth Orbiting Laboratory (Slide 1) and the Viking Mars Lander (Slide 2).

The most significant reason for applying system safety to these programs, and the reason which precludes the need for any debate, is past accident/incident experience. When we relate to the monetary loss of aerospace hardware that the nation has experienced during the last decade, it staggers the imagination. Part of this loss experience can be attributed to our early days of trial and error, when we were pioneering aerospace technology and at a time when international prestige was wavering because of the space efforts of other nations. Playing catch up is risky business and obviously risks were taken based on the availability of information at that point in time.

We have progressed significantly from this period of time as substantiated by the increasing number of space program successes. However, more ambitious projects require more exotic and complicated hardware. With the first manned flight came increased concern for crew safety, establishment of safety requirements and standards, and emphasis of safety to all program personnel. This was done with the knowledge that the crewman is capable of using judgment and would contribute to the decision making processes whenever a situation arose that encroached on the margins of safety provided in the design of the hardware or the operation. Manned space programs have one asset not enjoyed by unmanned space programs; this is the crew member and his abilities to observe, assess and rationalize system malfunctions or unscheduled events during the course of the mission. I would like to defer any reference to specific unscheduled events or accidents that have taken place; however, to make a point very clear as to the value of this asset reference is made to the flight of Apollo 13. Specifically, the capability of crew members to establish a lithium hydroxide system as a part of the life support system when standardization of lithium hydroxide canisters for all crew quarters, LEM and Command Module, was not a part of the system design. This was an onboard fix and was in part a real contributing factor to decreasing the risk associated with crew survival.

To present the degree of system safety application that is considered essential to the safety of mission objectives, for both programs, consider first the common aspects and then review the details and differences that are required for the individual programs.

The safety objectives common to both manned and unmanned programs are:

Initial System Safety Planning
1. Understanding the program objectives.
2. Identify gross hazards associated with the hardware concept. (Gross Hazard Analysis)
3. Establish baseline safety design criteria.
4. Draft the system safety program plan commensurate with the program objectives.

The Design Phase
1. Analysis of systems and subsystems.
2. Detailed safety design requirements.
3. Hazard reduction program.
4. Management visibility to risk.
5. Flight crew procedures.

The Hardware Build and Test Phase
1. Review of procedures (manufacturing and test).
2. Test crew certification and training.
3. Review of tests' data.
4. Launch procedures' review.
5. Launch operations (KMI 1700.1 and AFETR 127-1).
6. Flight procedures.
7. Crew Training.

The Mission Phase
1. Contingency plans.
2. Emergency procedures.
3. Simulations.

Having considered the commonalities, we have to come to one conclusion and that is; the technique is the same. The real difference lies in the degree and requirement for applying the techniques to the individual programs. Looking at the Program Planning Phase we find the following:

Initial System Safety Planning

1. Understanding the program objectives.
2. Identify gross hazards associated with the hardware concept. (Gross Hazard Analysis)
3. Establishing baseline safety design criteria.
   (a) Design Handbook (AFSC/NASA DH 1-6 and DH 1-X).
   (b) NASA Accident/Incident Summaries.
4. Draft the system safety program plan commensurate with the program objectives.

In the unmanned program the crew is essentially the science committee and Mission Control on earth, and all efforts are concentrated on obtaining scientific data through the use of automated spacecraft. Therefore, the role of system safety must interface with the science authority to the extent necessary to acquaint the scientist with the fact that system failure of hardware designed to launch and deliver science experiments to their destination is as important as the experiment itself. Further, it must be understood that the data acquisition of science hardware is still the scientist domain; however, the mechanisms that deploy it, energy and power for it, as well as the communication link between experiment and earth, interface with transporting hardware and therefore becomes a matter for system safety as well as engineering. However, with a manned system the crew consists of the Flight Crew and Mission Control and the safety effort concerns itself with protecting the crew as well as the scientific objective of the mission. System safety that is concerned with a manned system must understand the crew complement, the mode of operation of the crewman; i.e., suited/unsuited, IVA/EVA and, in general, what tasks the crewman will be required to perform. To be more specific in this area, what task will require a suited mode. Is there a requirement for a fire extinguisher system and caution and warning system; what requirements are specified for material controllability (such as, NASA Document No. MSFC Spec 101B, "Spec Flammability, Odor, and Offgassing Requirements and Test Procedures for Materials in Environments which Support Combustion"), and any other program objectives or mission constraints.

During this initial planning phase, system safety must identify the gross hazards associated with the conception design of the hardware and the preliminary mission planning. The gross hazard analysis is a requirement that must be accomplished by both the manned and unmanned missions. It is performed to obtain the initial safety evaluation of the program. The primary objective is to provide the basis for subsequent system safety task, safety criteria and other requirements that must be established.

When the gross hazard analysis has been evaluated, safety must generate the baseline safety design criteria to be used during the detailed design phase. Since, at this point in time, we should know what the conception design will be we can now review the AFSC NASA DH 1-6, DH 1-X, and the NASA Accident/Incident summary documents to establish our baseline safety design criteria. If we have criteria availability problems, we may use the AFSC NASA DH 1-6 information sources listings. Through this listing we may contact knowledgeable people in the technology field of interest for new criteria being developed in laboratories that may be useful to our program. After having developed an understanding of the above data we now can generate a system plan that is commensurate with the program objectives which is cost effective and will provide us the safety necessary to mission success.

The Design Phase

1. Analysis of systems and subsystems.
   (a) Baseline.
2. Detailed safety design requirements.
   (a) Update baseline incorporating program peculiar criteria.
3. Hazard reduction program.
   (a) Hazard Catalog.
   (b) Safety Assessment Reports.

4. Management Visibility to risk.
   (a) Design Reviews (PDR, CDR).
   (b) Management Reviews.
5. Flight crew procedures.
   (a) Mission Rules.

When the program enters the design phase the safety engineer begins updating and expansion of the gross hazard analysis that was conducted during the initial program planning. Many references are available on the types of analysis which are applicable to this expansion. When the system safety engineer understands the mission of the unmanned program, he is in a better position to select the safety analysis method most applicable to the science package and all of its ramifications as it effects microbiology, terminal sterilization, and the varying degrees of hazards introduced by fully encapsulated spacecraft which are armed, loaded and pressurized prior to reaching the launch pad. Risk and hazard assessment play an important role since you can no longer depend on procedurally controlling hazardous configurations and the introduction of hazardous materials or devices as late in the countdown as possible. System safety risks are now beginning to present themselves at the laboratory and it is at this point in time that effective system safety analysis and the conclusions of those analysis can preclude potential hazards evolving later in the program. Therefore, safety priorities are established for the hardware used to acquire scientific data as well as the hardware and operations that will deliver it to its destination.

The scientific community identifies what it wants to accomplish, where on the planet it can best make its acquisition, and what it believes the results should be. To get them there becomes the challenge confronting engineering. Engineering now has to work the problems of transporting and deploying the science package and this includes, providing the capability to automate and control the spacecraft to its final destination and to support the life cycle requirements of the scientific objectives. The system safety role for unmanned space programs now must consider the hardware and operational interfaces associated with both the role of science and the role of engineering. Although the system safety analyses of subsystems and systems are common to both manned and unmanned programs, it can be identified that the degree of analyses and the tradeoffs on the analytical results that identifies hazards are somewhat different. Redundancy for precluding single failure points on critical spacecraft system operating modes becomes a priority since crew participation is not available. Therefore, all critical or catastrophic hazards identified must be eliminated because the degree of risk is unacceptable for mission success. Onboard repair and/or flight plan revisions are not a negotiable tradeoff for unmanned flight and this dictates that system safety analyses consider the system reliability criteria to be verified during environmental testing and qualification and checkout of systems when categorizing the hazards identified as a product of the analyses that are performed. The significant point to be made here is that system safety engineers must recognize and understand the success criteria for environment and qualification testing of systems and that such criteria is equivalent to or exceeds the safety of design requirements or margins to insure the system is not unsafe and will not in itself be the cause of mission or mission objective loss.

The system analysis that is selected for the manned program must provide a smooth transition into the operational hazard analysis used during the operations phase of the program. This requirement is a must to insure that hazards identified during the design phase that cannot be removed by design can be flagged until they are solved by procedure and/or caution and warning systems. As an example, the next two slides (3 and 4) show an experiment on each of the programs (Viking and Skylab). The Viking soil sampler must work every time, and if it does not, there is no one to fix it. However, the Skylab Experiment T025 extends through the Scientific Airlock of the Workshop and if it cannot be retracted a flight procedure provides for a crewman to jettison the extension boom overboard. Hazard reduction programs are essentially the same for both types of space missions. However, with unmanned missions you have the added responsibility to consider long term transcruise modes to planets. (For example, Viking is 360 days.) This aspect is a serious consideration of science,

management and engineering and should be as important to the safety role when searching for system hazards and providing recommendations for the reduction of hazards or risks to the mission. Will it work when it gets there is the responsibility of engineering, but will it work safely is still a priority and system safety should apply the "what if" technique and make a contribution by revealing any discovery of potential hazards to the responsible design engineering agency. Earth bound accidents have been caused by some rather unique nonoperational conditions. Stress corrosion, decomposition of materials during long term storage, and ordnance explosions, to cite a couple of examples. These examples are of the obvious types; however, system safety engineers make a contribution by ferreting out the not so obvious conditions that could cause accidents and this is a very significant system safety role when you consider the length of time associated with the unmanned mission versus manned missions. The reduction of hazards can be substantial providing early identification can be accomplished. Therefore, system safety analyses and hazard reduction programs are interdependent and you cannot be effective by accepting one and not the other. There is an old adage; "Where there's smoke, there's fire," and so with unmanned aerospace systems there is always good reason to be concerned about that which you cannot manually control or have visual observation and human capabilities to secure before the not so obvious becomes the obvious.

As the safety analysis progresses, new requirements are necessary and at this point the updating of the baselined design requirements must be accomplished. If this is not done problems that have been solved continue to appear causing much effort in looking for solutions.

This approach results in the system safety discipline engaging in the task of establishing safety requirements and margins based on what needs to be done or what will be done rather than being totally engaged in monitoring for inclusion of existing requirements. These design safety requirements are extremely important when you consider that each spacecraft weight saving made during spacecraft design development is an opening for inclusion of additional science experiments and this substantiates the reason for the interfacing of system safety with the scientific community.

With the safety analysis and design requirements completed for basic design reviews the operating methodology for hazard identification and control is done in two different ways. For the unmanned program the Hazard Catalog (HC) is used as a summary of the hazards that have been uncovered by the analysis and have not been solved. The manned program uses the Safety Assessment Report (SAR) to evaluate each hardware system. Why the difference - the unmanned program is usually very complicated, but uses very few contractors, one procurement agency, and all of the hazards can be cataloged in one document; whereas, the manned program, Skylab, has four major modules, sixty experiments, and over 20 contractors, working with five NASA centers which makes it much easier to use the Safety Assessment Report.

The design reviews (PDR, CDR, TDR) is the place where the SAR and HC are reviewed with the hardware design to assure all hazards have been identified and action taken to correct those identified as catastrophic (see Mil-Std-882). The remaining identified hazards are presented with recommendations for correction. The correction can be a redesign, a safety device, or procedure controls. Here caution should be taken in the unmanned program, a procedure fix is nearly always ruled out, a safety device should be used with caution since it may have to be removed, therefore, either redesign or accept the hazard and assure it is flagged in the hazard catalog.

The flight procedures are now considered and if this term is used to include the ground (Mission Control) and Flight (Crew) procedures, it can be seen that both programs need the Mission Control procedures; whereas, only the manned program require the Flight Crew procedures. Taking the SAR, HC, and outputs of PDR's, CDR's and TDR's we must see that they are provided as initial input at this time to these procedures.

Progressing through the development of the programs the next phase is the;

Hardware Build and Test Phase (Slide 11)

1. Review of procedures (manufacturing and test).

2. Test crew certification and training.
3. Review of tests' data.
   (a) Special Test (Vacuum Chamber).
   (b) EMI - Environmental.
4. Launch procedures' review.
5. Launch operations (KMI 1700.1 and AFETR 127-1).
6. Flight procedures.
   (a) Emergency Procedures.
   (b) Contingency Plans.
7. Crew Training.
   (a) Simulations.
   (b) Training Hardware.

The procedures that will be used during the build and tests are subjected to a safety review regardless of the type of program. In most cases these procedures are reviewed by both System Safety and Industrial Safety engineers. Another area that is considered is the training and certification of the personnel that will manufacture, test and checkout the hardware.

The training of personnel required for manufacturing, handling, inspecting, testing, and launching of space programs assures their capability for competently performing the required program functions. The certification encompasses system knowledge, training course completion, adequacy of individual and crew capabilities. To assure product integrity through all phases of development, test, and operation, it is mandatory that all activities which contribute to program success are performed by certified personnel.

Mil-Std-882 recognizes the importance of operational and maintenance personnel training and crew qualifications and certification by requiring them as part of the sytem safety program.

Proceeding into the test program the safety engineers are concerned with the tests' performance and the data derived from same. Specifically, special tests such as, vacuum chamber, simulations, aircraft zero-g (KC 135), vibration, etc., are tests where the safety engineer can learn much about the hardware that is not built. The tests can validate the criteria that was used, and more importantly, the data can assure that the procedural requirements to be imposed during launch and mission are valid.

System safety has now progressed from the initial program concepts to hardware that is built and tested and now ready to perform the mission.

The hardware is now transported to the launch center to be mated with the launch vehicle. If the safety engineer has performed his tasks throughout the program this becomes a routine step, however, invariably it is found that someone has not complied with KMI 1700.1 and/or AFETR 127-1 and many problems now occur with Range Safety. It is imperative that compliance with the range documents begin during the hardware design and continue throughout the program. The requirements for the unmanned program should be subjected to a very strenuous review due to the fact that many times ordnance must be installed, pressure systems require charging, and power systems must be hot prior to movement to a launch pad. Usually the manned program does not require these hazards to be introduced until the countdown for launch has begun.

The launch and flight crews have been in training for quite some time at this point; however, the training and simulations become much more strenuous during this period. The emergency procedures must be validated, through simulation, and finally corrections made. The contingency or backout procedures have to be practiced and finalized. This is the time that system safety checks the HC or SAR to assure all hazards that have been identified during the program are closed. The closed action may be redesign, procedure or program decision to fly with, regardless of how all items must be closed out. Now, and only now, is system safety ready at the Launch Readiness Review to report to program management that vehicle is safe and ready to commit to the mission, with known safety factors and in the cases where total close out of the hazard has not been accomplished, the degree of risk that is being accepted.

Management visibility to non-acceptable, as well as acceptable risk, is in the final analysis the product of an effective system safety program for either the manned or unmanned program. Rarely has management overlooked high risk areas of inherently hazardous materials, systems or operations, when identification of the hazards were made

known and the proper controls, required procedures, and devices were provided to control the risk. Conversely, management has been a victim of high cost losses and liabilities due to phenomena that was not controlled because of lack of information on risks, and cost constraints where the hazards are not identified early in the program.

The mission phase now becomes another major step, and the difference between the two programs are extreme.

The Mission Phase

1. Contingency plans.
2. Emergency procedures.
3. Simulations.

In reviewing our two programs (Skylab and Viking) for their particular missions we find that the initial launch of Skylab is in reality an unmanned program. The Workshop is launched and mechanisms must operate, such as, the Apollo Telescope Mount (ATM) must unfold from the stowed position to the operational position, without a crew aboard to make any visual observations, or take any corrective actions. However, if the deployment systems were to malfunction there still remains the contingency plan whereby the crew may be able to rendezvous with the laboratory and fix the malfunctioning part of the system. This is where our simulations are so important because we could simulate the actions to repair the system on the ground before launching the crew.

Considering a similar case for the unmanned program where no crew is programmed to rendezvous if the systems did not work the total mission would probably be lost. For instance, considering Viking, if after launch and the long term transcruise to the planet, the orbiter and the lander did not separate properly, we would in all probability lose the entire mission. Some contingency planning, redundancy in the unmanned systems is possible, however, there is no alternative for the benefits of crew member/equipment interfaces.

In order to compare the manned versus unmanned programs, a summary of the differences is in order.

1. The safety programs consist of essentially the same elements.
2. The real difference are the tools used and the extent of application.
3. Both programs require safety to begin in the conceptual phase.
4. The unmanned program requires more interfacing with the science community than does the manned program.
5. Both programs require design requirements.
6. Hazard analysis is a requirement of both programs; however, the method of presentation of the results is different:
   Manned --Safety Assessment Report
   Unmanned--Hazard Catalog
7. The manned program does require a review of crew procedures and flight training requirements where the unmanned does not.
8. The mission phase is entirely different, whereas, the manned program does require flight contingency plans and emergency procedures, the unmanned program does not.

In conclusion, it is quite evident that the system safety principals applied to both programs are a contributing factor to mission success. The discipline certainly has more than adequate support of top management, and the results are effectively implemented at the hardware build and test level by technicians once the system safety requirements are known. The key to its success, however, is the middle management acceptance and endorsement. Design engineering, planners, project engineers, systems managers, etc., can and will inhibit a successful system safety effort if they don't understand the following:

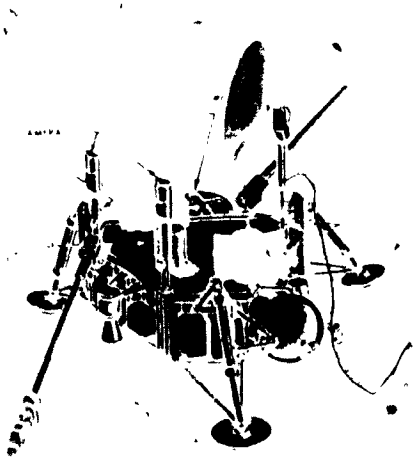
1. System Safety objectives.
2. System Safety differences as it relates to Quality Control, Reliability, and maintainability.
3. System Safety as a contributing check and balance against oversights.
4. That successful program management responsibilities includes hardware safety and they should avail themselves of the results of the system safety tasks.

It has often been said; "We always have the assets and resources to do it the right way

the second time - why not do it right in the first place." System safety, when it is permitted to function, is cost effective, contributes to mission success, and is a needed discipline. If it is not, then industry and government are going to have to continue with programs of accident and risk correction, not accident incident prevention or risk control. There is a lot at stake on Skylab and Viking that cannot be measured in dollars and cents. National prestige, lives of crewman, and scientific data that may hold the key to man's very existence - what a price to pay, for just one accident or mission failure that is within the realm of our ability to predict, take action to correct and to control the level of risk we must take to progress to the next plateau of space exploration.

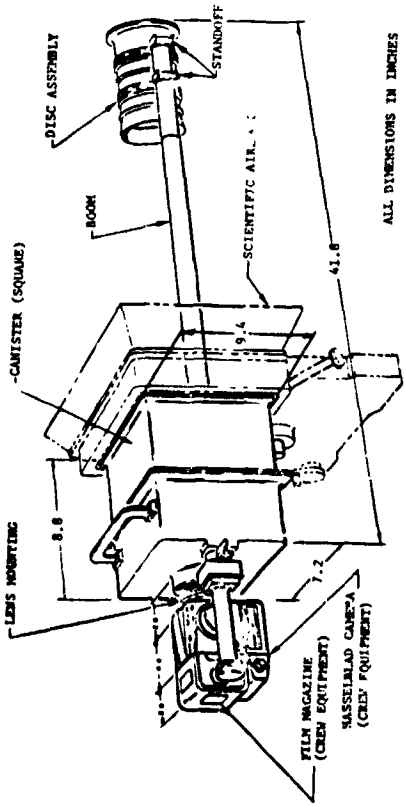
SLIDE 2

VIKING



SLIDE 3

VIKING LANDER



SLIDE 4

T025 EXPERIMENT

CORONOGRAPH CONTAMINATION MEASUREMENTS

N72-25980

THE REDUCTION OF A "SAFETY CATASTROPHIC" POTENTIAL HAZARD - A CASE HISTORY

by

Joseph P. Jones

The Bendix Corporation
Aerospace Systems Division

Presented at the

Second Government/Industry
System Safety Conference
Goddard Spaceflight Center
Greenbelt, Maryland

May 27, 1971

Early this year, the fundamental design concept of the Lunar Seismic Profiling (LSP) Experiment was challenged when a mode of operation on the lunar surface was identified which could conceivably result in the detonation of high explosive charges before the departure of the Apollo 17 astronauts. As a quantitative analysis of the problem was beyond our capability at the time and as the effects of an explosion on the lunar surface are unpredictable from a safety viewpoint, we found it necessary to report the problem to the Manned Spacecraft Center as potentially "Safety Catastrophic" as defined by NASA directive and by our own LSP System Safety Plan.

In this paper, I will attempt to track through the sequence of events, mainly as they relate to the system safety discipline, which resulted ultimately in the reduction of this potential hazard to "Safety Negligible." For the sake of brevity, I have minimized the discussion of the test results and some of the second order effects related to the operations of the hack watches.

The object of the LSP (Figure 1) is to utilize artificially induced seismic energy to investigate the physical characteristics of the lunar structure. It will be deployed on the surface of the moon during the Apollo 17 mission. Eight packages containing explosive materials ranging from 1/8 to 6 pounds will be set out at distances up to 3.5 kilometers from the Apollo Lunar Surface Experiments Package Central Station which will be erected near the Lunar Module. The packages are activated by the astronauts as they are set out by removing pull pins which initiate internal timing functions. (Figure 2)

From a safety viewpoint, the key components of each explosive package are the timers, two per package, which establish the conditions permitting the conversion of a firing command from the Central Station into the detonation of an explosive package after departure of the astronauts from the lunar surface. The timers are completely mechanical and each contains a modified military "hack" wrist watch movement which controls the advance of a timing drum to a position where the output function is initiated. The timers are preset and there are no controls or adjustments to be made during the mission. It remains only for the astronauts to remove four pull pins to start the watch movements and to remove the mechanical, redundant inflight safety features when the packages are in position on the lunar surface. (Figure 3).

When the safe/arm timer actuates, it moves a slide from a position in which it provides complete physical isolation of the end detonating cartridge (EDC) from the explosive block to a position in which a hole in the slide lines up to expose the explosive block to the EDC. This provides a propagation path to detonate the package. If for any reason detonation does not occur and the package is still intact after two hours, the timer will cause the firing hole to slide past the EDC, thereby permanently isolating the EDC from the explosive block.

One hour after the safe/arm timer opens the firing time window, the battery timer releases a firing pin which strikes a percussion primer in a thermal battery. The heat generated within the battery as a result of this action liquifies a normally solid material, creating an electrolyte which activates the battery for a period of approximately three minutes. With power applied to the receiver, decoder, and capacitive firing circuits, the explosive package is capable of responding to a firing command from the Central Station.

Early in the preliminary design phase of the timers, it was recognized that environmental conditions to which the watch movements would be exposed on the lunar surface would cause an increase in the amplitude of their balance wheels; this could cause "overbanking" and result in large timing errors and premature initiation of the timer functions.

The terms "balance wheel amplitude" and "overbanking" are fundamental to the problem and require a short description of the operation of a mechanical escapement watch movement (Figure 4) such as most of us still wear on our wrists. It should be made clear that tuning fork and quartz crystal regulated movements, which we all will see more and more or as time goes on, are not pertinent to this discussion.

Timekeeping in a watch movement is actually performed by controlling the rate of dissipation of energy from the coiled mainspring through a gear train. The control function is provided by the balance wheel and hairspring

assembly which, when properly adjusted, oscillates in simple harmonic motion. The timer hack watch, per common practice, oscillates at a rate of five times per second.

To define the terms previously mentioned, the measurement of angular displacement of a point on the rim of the balance wheel as it osciliates is the "amplitude" and is measured in "turns." The amplitude of a given watch movement is a function of its mainspring torque characteristics and is not adjustable. The maximum amplitude in any watch movement must be less than that which would cause the balance wheel to come around full swing and contact the escapement from the opposite direction. If this were to occur, the harmonic motion of the balance wheel would be disturbed by the rebound off the escapement and the rate would increase, causing the movement to run faster than normal. This condition, known as "overbanking," is never encountered in a normally operating watch here on Earth.

However, we have reason to suspect that astronaut wrist watches overbank. In an unofficial poll conducted at our request, when this problem first arose, most of the astronauts who were questioned responded that they noticed a tendency for their watches to run fast during a mission, and one was willing to estimate approximately plus twenty minutes per day. We might also note that, typically, the maximum possible amplitude of a fully-wound watch would be 1 3/4 turns and the operating amplitude would be 1 1/2 to 1 5/8 turns with the balance wheel axis vertical (watch lying flat). With the watch on edge, the typical amplitude would be 1 1/4 to 1 3/8 turns due to increased balance staff pivot friction in this position.

In most instrument applications of watch movements, the primary concern is not the amplitude of the balance wheel but the rate of the watch; whether it runs fast or slow, and how much. The designer is free to allow the amplitude to fall within a rather large range as it has only a second order effect on rate.

In the LSP Timer, where safety and reliability are of the utmost importance, highly precise timing is the second-order requirement. We have determined that balance wheel amplitude, rather than rate, is the more important factor due to the unusually wide range of environmental factors under which the watch is required to perform, and by the fact that there are upper and lower limits to usable watch amplitude.

The lower limit which we have not as yet discussed is not a precisely fixed point but an ill-defined area of poorer and poorer operation as the amplitude decreases. This is a condition which we earthbound people can relate to as this is exactly what happens to our watches when we fail to take them in for periodic cleaning. The lubricant gums up, the internal resistance of the mechanism increases, and, as there is no compensating increase in mainspring torque, less energy is transferred into the balance wheel and its amplitude decreases. This results in due course in noticeably large timing errors, erratic operation, and ultimately, inability of the watch to run at all. Low temperature has the same effect in that it causes the watch oil to congeal.

When the overbanking problem was originally presented to us by the timer subcontractor, they were unable or unwilling to predict the magnitude of the resulting timing error. They would only say that the watches could conceivably run "several times faster than normal". The main reason for this conservative approach probably was their total lack of quantitative information on the effect of the lunar gravity.

On our part, we had established a nominal 90-hour runout time requirement in order to maintain a 1.5 safety factor, or thirty hours, between the contingency lift-off time of the LM and the detonation of the first explosive package. We viewed any significant inroad on the safety margin with alarm and, for a time before we could put everything in proper perspective, were fearful that we did not have a viable design concept. The steps that we went through in getting to where we are today are noted in Figure 5. Each will be discussed briefly in turn.

The subcontractor had little difficulty in verifying that the problem was a real one. There was test experience from other programs to draw on which indicated that temperature and pressure were factors and the condition was demonstrable by the application of excessive torque to the mainsprings of randomly selected watches through their winding stems. You are all welcome to duplicate

this experiment on your own watches, but see your local watch maker, not me, if you shear off your winding stem.

I would like to show you at this point the form used to document this problem (Figure 6) within our program. Although the concept for the form and its format is my own, most of the checklist items are the work of Mr. J. Richey of Bellcomm, Inc., and were taken from a paper presented by him to the Washington Chapter of the System Safety Society on June 19, 1969. Normally, this form is used as a rough worksheet and has two purposes. First, it is intended to stimulate the imagination both of the System Safety Engineer and whomever he is trying to extract information on a problem. Second, it provides some kind of record of all the chaff we sift through in evaluating a problem, particularly the negative ones which are otherwise not documented. The form has been reasonably successful and has been adapted to other areas than manned spaceflight.

It seemed prudent, after overbanking was verified as a problem, to review alternate methods of providing the timing function for the LSP. Other methods had been considered and rejected in trade-off studies from which the selected design evolved. In the light of an overbanking problem of unknown magnitude, they might have appeared more attractive on second look. I won't belabor this effort, for all the potential candidates were still unattractive for various reasons, primarily weight and reliability. However, none could have scored as high on safety as the concept of two completely independent mechanical timers that could be initiated only by the astronauts during EVA. For once, the requirements of safety, weight, reliability, and volume were entirely compatible. We were convinced that we had the best design, if we could resolve the overbanking problem, and that a change at this point would guarantee nothing other than schedule slippage and cost overrun. We then chose to move on to the next step - to experimentally evaluate overbanking.

It was originally predicted that amplitude would increase on the moon because of high temperature, high vacuum, and low gravity. Experimental determination of the effects of temperature and pressure was a relatively routine matter except for the necessity to adopt a state-of-the-art fiber optic instrumentation system to measure balance wheel amplitude to the order of accuracy required.

The real problem was in the evaluation of the effect of reduced gravity. It was known that balance wheel amplitude changes when the watch is changed from an edge position to a flat position because of changes in bearing friction. From this it could be inferred that the effect of gravity which would cause a similar change in bearing friction is not negligible and that a substantial increase in balance wheel amplitude over the nominal earth value could be expected when the watch was operating on the lunar surface. The question was, How much?

A centrifuge test was initially performed to provide g vs. amplitude data in the approximate range of 1 to 10 g and extrapolate backward to the lunary 1/6 g area. Not being convinced that this procedure was entirely valid, additional test methods were sought for cross-correlation.

As a result, two other methods were proposed - low or zero g flights in the C-135A aircraft operated by the United States Air Force as a zero g test and research facility and in the 500 foot free fall zero g research facility operated by the NASA Lewis Research Center. Tests were ultimately performed at both facilities under the sponsorship of the NASA Manned Spacecraft Center, the procuring agency for the LSP Experiment.

Although none of these three test approaches were in themselves completely conclusive, they all pointed in the same direction - that the increase in balance wheel amplitude under the influence of lunar gravity was no greater than one quarter turn. We thought at this point that we had the most important variable under control but, in fact, the most significant fact to be uncovered in the investigation was to come when the effects of pressure and temperature were investigated.

The results, of these tests as presented in Figure 7, substantiated the trend indicated in the initial tests, and a significant break point was found to exist in the 1 torr range. The maximum effect at 180° F, 1 torr, results in an increase in amplitude of approximately 1/4 turn. At the ambient temperature (approximately 75° F) only one of the three test

4-5

movements showed any appreciable change in amplitude (1/8 turn). However, beyond 1 torr the slopes increase sharply and in the hot case, extend into the overbanking region.

Another surprise was that our test results did not substantiate the traditional horological theory that aerodynamic damping significantly contributed to the total internal resistance of balance wheel system. This case had been so strongly made in our early discussions that a streamlined balance wheel was actively considered at one point as a partial solution to the overbanking problem. Although our data in the range of aerodynamic interest is scattered and somewhat questionable in an absolute sense, the general slope of the curve as it approaches 1 torr is unrefutable and indicated that the change of amplitude is less than that which an expert watch maker can observe.

The significant conclusion to be drawn from these tests is that, although maintenance of one atmosphere of pressure within the control module cavity is desirable for other reasons, non-catastrophic leak rates down to a minimum pressure of 1 torr during lunar operations have no great significance to the overbanking problem.

The results of holding pressure constant and varying temperature correlate. Two series of tests were performed, at ambient pressure and in the range of 1×10^{-4} torr. The summary results, corrected to eliminate torque variations due to mainspring wind down, are presented in Figure 8.

The effect of reduced pressure on the results of these tests are dramatic. Whereas a sharp point of inflection is displayed on the ambient curve in the 40-50° F range which renders amplitude essentially independent of temperature above this point, the vacuum curve rises steadily at a nearly constant rate and could cause a fully wound watch to overbank above 150° F. This is demonstrated by the points plotted above the 1 3/4 turn line, a physical impossibility as the balance wheel amplitude cannot increase beyond the point of overbanking. These points result from large corrections on measurements made after the vacuum chamber (and the watches) ran over night to get down to test pressure. It may be inferred that, had the measurements been made immediately after winding the watches, overbanking would have been observed in at least two of the test watches.

The close grouping of the data at the cold end of the curve suggests that pressure has little effect on amplitude at low temperatures but that there is almost a straight line relationship between temperature and amplitude in the range from stoppage at -35° F (-20° F in a vacuum) to the point of inflection at 40-50° F.

The final piece of information needed to evaluate the overbanking problem was related to mainspring torque characteristics. Mainsprings provide higher torque when fully wound up, and less as they run down. A characteristic torque curve is shown in Figure 9. The erratic torque variations at the high end of the curve are eliminated by the use of a recoil click in the winding ratchet mechanism which releases a few ratchet teeth before it locks the mainspring ratchet after winding. The low torque of the low end is eliminated by providing a longer mainspring run than is required for the mission involved. The resulting torque variations are thereby reduced to account for an amplitude variation of approximately one quarter of a turn.

Tests were conducted measuring torque as a function of mainspring wind as expressed in number of turns of the mainspring barrel. This information was used in correcting other test data to eliminate torque variation due to mainspring position, and to establish a representative slope, which turned out to be 4.4, to use in the presentation which follows. It should be mentioned here that the test watches used in this investigation were "set down" to a nominal one turn amplitude by substituting a convenient available mainspring from a smaller watch in the subcontractor's product line. The scope must be reverified in the 140 hour mainspring with which the production timers will be equipped.

Figure 10 shows the method by which the test results were put together to arrive at D and E conclusion that overbanking is not a matter of concern during normal operation of the LSP timer. Normal operation of course, means a condition in which seal integrity is maintained and the watches are operating at a nominal pressure greater than 1 Torr. As the O-Ring seals, three in number, constitute single point failures the next step was

to determine the worst resulting timing error on the safety of the astronauts and on the probability of success of the experiment.

This was accomplished by overbanking a watch under controlled conditions and measuring the resulting change in rate. By varying the controlled condition a curve was constructed of change as a function of overbank from which reliable predictions could be made. This curve is presented in Figure 11.

On the left side of Figure 11, it may be seen the application of a known torque to a fully wound down mainspring barrel resulted in the winding of the barrel to a point of equilibrium at which a certain balance wheel amplitude was attained. As the torque was increased incrementally, the barrel wound up further and the amplitude increased in a predictable manner. When the barrel was fully wound the amplitude continued to increase as a function of applied torque until the maximum amplitude was attained and the balance wheel overbanked. Up to this point there was no timing error measurable with a stop watch.

The curve continues on the right side of the figure but now, with the maximum amplitude attained and the watch running overbanked, the error rate becomes the dependent variable. Figure 12 repeats this portion of the curve as well as similar results for the other two test specimens.

As amplitude has thus been demonstrated to be a function of torque, the incremental increases in amplitude previously discussed can be converted to equivalent values of torque and, if combined in a rational manner, the resultant can be read out on the worst case curves in Figure 12 as a reasonable estimate of the worst timing error to be expected during lunar operations. This has been accomplished using graphical methods not discussed herein to account for the non-linearity of the torque curves in the overbanking range and to introduce a factor in the temperature effect based on the ratio of lunar gravity amplitude to earth gravity amplitude. Also accounted for and not previously discussed is the effect of an explosive package falling over on its side. After deployment the accumulative total of these worst case conditions is expressed as a maximum of 1750 grammillimeters of equivalent torque which may be converted to a maximum error of +120 minutes per day.

However, the two watch movements in a LSP package are aligned in planes at right angles to each other and only one of the two timers will be lying flat when the package is lying on any side. Thus the overbanking condition would be applied to one of the two timers. This failsafe condition would tend to cause a dud rather than a premature explosion since the timers must both be within their respective time windows for the firing operation to function.

Therefore, considering only a total seal failure as the worst case on edge condition, the maximum torque value is approximately 1480 gram millimeters or an effort of plus 40 minutes per day. Ignoring the decrease in torque over 90 hours, this works out to approximately 10% of the established 30 hour safety margin, and is the basis on which the potential hazard has been reduced to "Safety Negligible."

Although the worst case approach has sufficed to resolve our safety concerns, it does little to resolve the residual reliability problems. We are now at work developing a mathematical model of the balance wheel system to which we can apply our test results and predicted mission time line data to permit more meaningful analysis closer to the real case conditions which will actually exist. The O-Ring seal design is also under rigorous review at this time as a result of this investigation.

The remaining system safety task to be performed is indicated in Figure 13, which will ultimately become part of the safety assessment report for the LSP Experiment. We must establish the maximum torque and the slope of the production mainspring torque curve to assure lunar operation conforming to that presented in Figure 10. It is now important to establish tolerances on these numbers which will assure safe and reliable performance of the LSP experiment yet will have an impact on production costs and schedules no greater than required to achieve this goal. This is the sometimes forgotten system safety task which can not be overlooked in our ever more competitive industry. The system safety

engineer must be as cost conscious as all the other engineering disciplines and must see to it that no more effort is being expended in the name of safety than is necessary to achieve the desired results.

In closing, I would like to express my appreciation to several people; to Mr. Charles A. Sauter of the Bulova Watch Company and Mr. Rene' Besson of Ebauches S.A., (Neuchatel, Switzerland); to Mr. Jack Dye, The LSP Experiment Manager, without whose encouragement I would not be here; to Mr. Donald G. Wiseman, Manager of the Lunar Surface Project Office at the Manned Spacecraft Center for Authorizing the presentation of this material and to Bill Scarborough, who bears the responsibility for me being a System Safety Engineer.

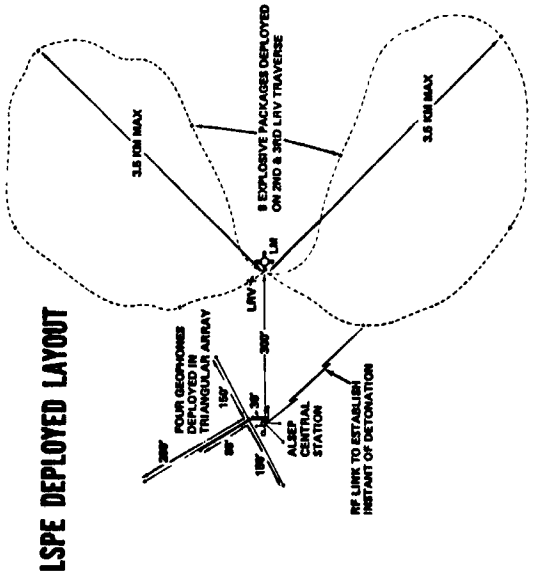


FIGURE 1

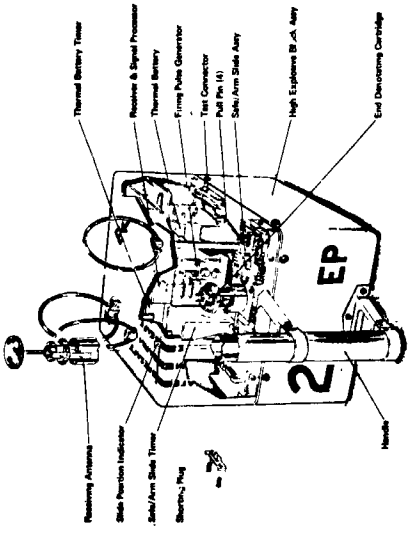
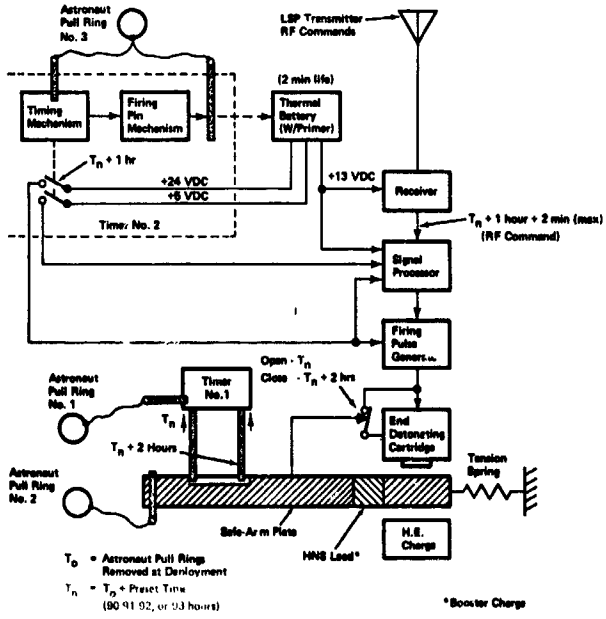
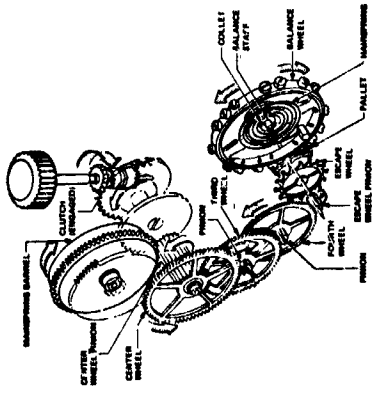


FIGURE 2



Block Diagram of Explosive Package

FIGURE 3



POWER TRAIN TYPICAL MECHANICAL ESCAPEMENT MOVEMENT

FIGURE 4

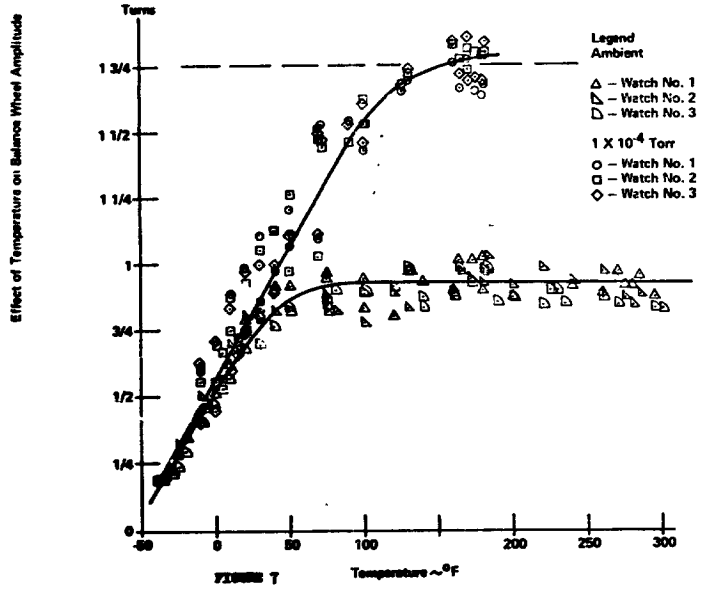


FIGURE 7

MAINSPRING TORQUE CURVE

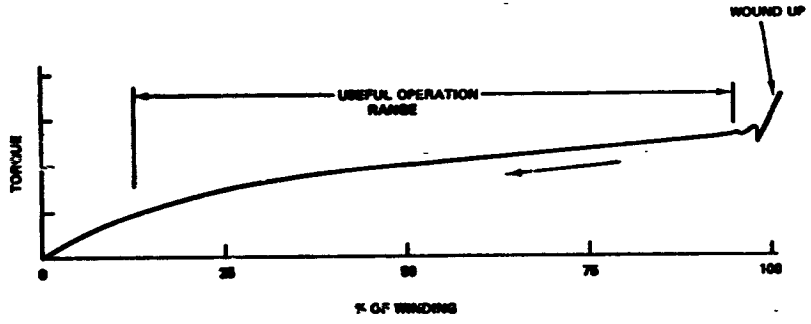


FIGURE 8

Bendix Aerospace Systems Division	SYSTEM SAFETY PROBLEM SHEET WATCH MOVEMENTS IN E & S/A TIMERS	Date 1-25-71 No. ___ of ___ Program ALSEP Array E LSP Author J. Imms
PROBLEM (1) COMPONENT FAILURE OR DEFECT 2. CREW OR GROUND PERSONNEL ERROR 3. CREW IMPAIRMENT	Watch Movements may "overbank" and run several times faster than normal under lunar environmental conditions of temperature, vacuum, and gravity.	
WHEN IN S/C 1. LAUNCH/CONTROLS ENROUTE 2. "DOCKING" LEM PROBABILITY EVENT OR FAILURE (3) OPERATIONAL ENVIRONMENT CREW RANGE	Potentially catastrophic event. Arming and power conditions may be satisfied prior to scheduled occurrence of firing event. The transmission of a firing command (central station in LSP mode) would cause a premature detonation, possibly before departure of LM.	
PRE-MISSION CAUSES (1) MAINTENANCE EQUIPMENT ERROR: DOES NOT MEET PERFORMANCE OR RELIABILITY REQUIREMENTS OR MISSION OR PREDICTABLE ENV. ON ENVIRONMENTS 2. MAINTENANCE MISSION PLANNING AND PROCEDURES 3. INADEQUATE PROTECTION AGAINST HANDLING OR HAZARDOUS ENVIRONMENTS BETWEEN EQUIPMENT AND CREW. 4. CREW ENVIRONMENTS. 5. DEFICIENCY OR INADEQUATE MAINTAINING, HANDLING, TESTING OR INSPECTION. 6. INADEQUATE SELECTION AND TRAINING OF PERSONNEL.	High initial balance wheel amplitude typical of good Earth practice would not permit increase in lunar environment without overbanking.	
PROPAGATION 1. NONE - MAINTENANCE CONTAINED (2) EXTERNALLY GENERATED STRESSES THAT PROGRESSIVELY REPAIR THE EQUIPMENT 3. EXTERNALLY IMPOSED STRESSES THAT PROGRESSIVELY REPAIR THE EQUIPMENT	4. INTERNALLY GENERATED STRESSES THAT PROGRESSIVELY REPAIR THE CREW. 5. EXTERNALLY IMPOSED STRESSES THAT PROGRESSIVELY REPAIR THE CREW.	Overbanking causes timers to run fast and to prematurely satisfy explosive package firing conditions.
CREW AND EQUIPMENT STATUS CREW A. UNAFFECTED B. IMPAIRED (C) INCAPACITATED	EQUIPMENT 1. UNIMPAIRED (2) MINOR DEGRADATION MAJOR DEGRADATION 3. INOPERATIVE	Effect of premature detonation not predictable. The worst case of incapacitation of the crew and/or the LM must be assumed.
MISSION IMPACT 1. CONTINUE MISSION 2. MODIFY MISSION 3. ABORT MISSION 4. RECOVER OR ABORT RESCUE (5) END MISSION	Neither crew nor Mission Control can monitor timer performance and would not be aware of the fact that a timer overbanked.	
END RESULT CREW A. SAFE (B) SAFETY COMPROMISED C. LOST	MISSION ACCOMPLISHED 1. ACCOMPLISHED (2) PARTIALLY ACCOMPLISHED 3. NOT ACCOMPLISHED	LSP Mission compromised by loss of one or more of eight explosive packages. Premature detonation of a package could still result in good seismic data depending on circumstances.

FIGURE 5

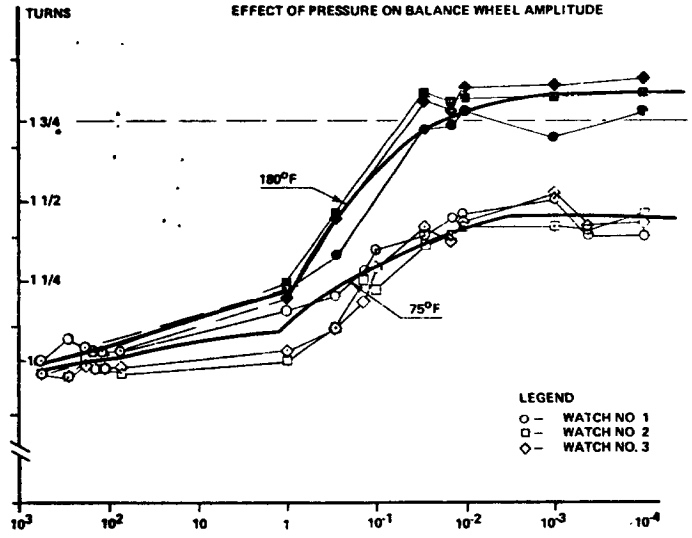


FIGURE 6

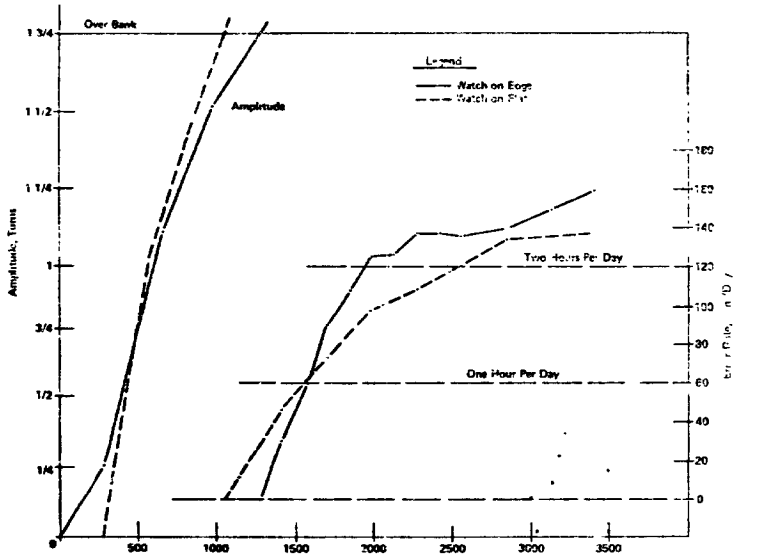
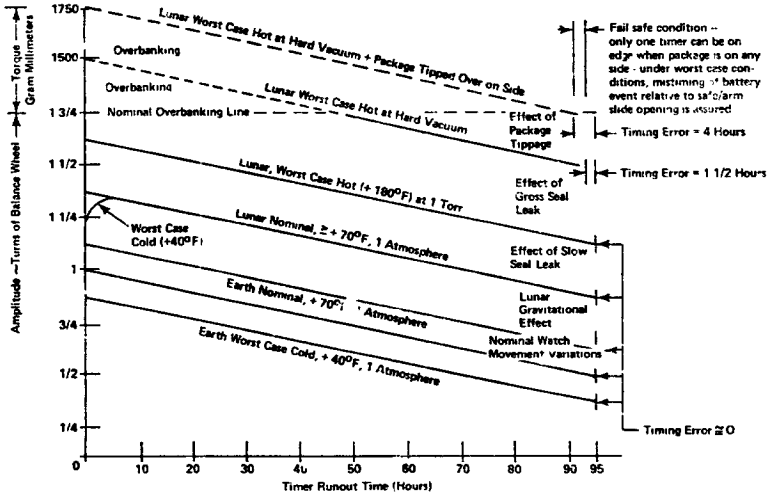


FIGURE 11

Amplitude and Error Rate vs Torc



Timing Errors Due to Changes in Balance Wheel Amplitude

FIGURE 9

Bendix Aerospace Systems Division

SYSTEM SAFETY RECORD SHEET

Item 5-28-8 Rev
Program ALSEP Array E
Name LSP
Phase Operational M, A,

SUBSYSTEM/TASK	SAFETY CONSIDERATIONS	HAZARD POTENTIAL	TECHNICAL APPROACH OR SOLUTION	CONTROL POINTS
LSP S/A and Battery Timers	Timer watch movements may overbank on the lunar surface due to cumulative effects of: 1. Pressure 2. Temperature 3. Lunar Gravity 4. Gear Train Error 5. Position	Negligible	1. Seal control module cavity at one atmosphere to eliminate pressure effect.	1. Mass spectrometer leak check to verify leak rate on subcontractor's ATP, i.e 10^{-6} atm. cc/sec maximum.
			2. Establish drag requirement for mainspring torque curve to produce balance wheel amplitude of ___ turns ± ___ turns fully wound, with a slope of ___ ± ___ between 8 and 100 hours of rundown.	2. Establish random torque curve for each flight unit during subcontractor's ATP.
	Timer watch movements may operate erratically during cold weather prototype and qualification testing due to low temperature effect on balance wheel amplitude.	Negligible	Auxiliary heating to be provided to assure minimum test temperature no less than cold case production for lunar surface operations (currently +40°F).	1. Field test requirements document. 2. Field test procedures.

FIGURE 12

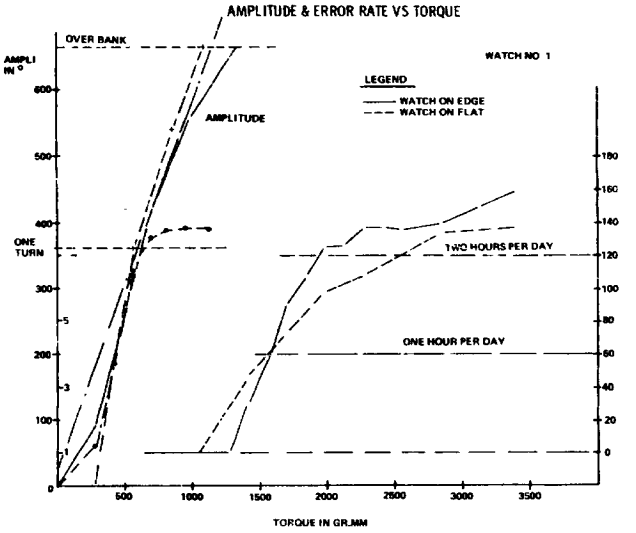


FIGURE 10

SESSION V

Questions & Answers

MR. REX GORDON: John Gera, where do you draw the line between what you consider industrial safety responsibilities and your operational industrial. Are the industrial safety responsibilities based on the talk that you gave?

JOHN GERA: That is a tough one but the line is pretty well drawn in the area of the manufacturing hardware itself--the machinery. We consider the machine and the man itself, that is industrial safety as we see it. We start looking at the detailed processes and the machine and the man. We sort of lap that over into the system safety activity.

REX GORDON: When you say machine are you talking about drill presses, etc.?

JOHN GERA: Yes, I am talking about the manufacturing machinery itself.

MR. GORDON: You mentioned that you had two plans. A system safety plan for operation and an industrial safety plan.

MR. GERA: "Standards"

MR. GORDON: "Standards." Who has the responsibility of the industrial safety standard, to prepare and implement it?

MR. GERA: The industrial safety standards are prepared by industrial safety people and the control or checking to see that they are adhered to is also the responsibility of industrial safety. I'll throw one kicker in here. No. 1 is that on a program, the industrial safety people work for the system safety manager in our activity.

MR. GORDON: They both report to the same manager?

MR. GERA: That's right, they all report to one man who is assigned to the Program Manager for safety. Sometimes we get into a little problem as to, is this the responsibility of industrial safety or is it the responsibility of systems safety. The point I want to make is that the job does get done whether it is by one party or the other.

MR. GORDON: One additional question. You mentioned that you had contingency plans for all conceivable emergencies, is that true? How much effort does it take to keep them updated? Do you make changes in the System?

MR. GERA: I stated that one way to do it is if you could identify every conceivable problem that you may have and when you do that then you would have to reduce that to what you consider credible and work on those elements. If I misled you there I apologize. You can't in my estimation plan for every conceivable problem that could go wrong--I don't see how you can.

MR. GORDON: Bill Scarborough, on the list of your functions, you start out with an analysis review, surveillance, tests and mission support. Do you have any function to give safety criteria into the program?

MR. SCARBOROUGH: I think that is inherent in the analysis function, that is the feed back into the design stage or design function. I am not sure that I understand exactly what you mean.

MR. GORDON: Where did the system safety effort start on the LEM Program? After the requirements had already been defined?

MR. SCARBOROUGH: We started very late, like about 3 years after the design was firmed up. We didn't really make much of a contribution to design, to basic design. We have been on-board for all of the design changes since we came into existence, and we do feed back into the sub-systems engineering groups.

MR. GORDON: Are you talking about coming on late with a formal program?

MR. SCARBOROUGH: Yes

MR. GORDON: I assume there was some safety on it before that.

MR. SCARBOROUGH: Yes there was a minimal effort.

W. H. SHAW (TRW): The comment about contingency planning reminds me that there is an important spin-off benefit to safety analyses that we find often gets overlooked. It could apply to matrix hazard analyses but particularly to fault tree which is really before the fact or prior trouble-shooting. In systems that involve maintenance planning, continuously operated manned systems and even one-shot systems that have activity at the cape, the output of the safety analyses is an extremely important and useful input to the trouble-shooting

procedures and maintenance manuals. We have found frequently that this is a real important spin-off that gets overlooked.

BOB ROSSI (GSFC): Mr. Don Ward and Mr. George Mumma indicated a certain flexibility in the system safety analysis which was tailored to the mission and (please keep me honest if I am misquoting), however, in George's presentation, I thought I detected an inflexibility at the point where he mentioned with respect to launch operations when he talked about 127-1 and 1700-1 and I am wondering, I have run afoul of these many times myself, what are your views regarding these documents, why shouldn't they be a little flexible?

DON WARD: They are flexible really. You can get waivers but you have to show them where you need it and you have to show them that you are still safe. I don't think that these documents are necessarily the only safe way of doing something, and we have a couple of systems that we are going to ask for waivers on. One is a premature separation destruct system. We don't want to carry a destruct package all the way to Mars, and we think that we can show them that if this spacecraft should separate prematurely the engines cannot fire and it would follow a ballistic trajectory into the ocean. Hopefully we can get a waiver on that. I think from a mission standpoint we will be safer without it than we would be with it; and I think to answer your question, those documents are not inflexible, but you have to have a good reason for changing the way of doing business with them.

QUESTION: A question for Mr. Jones on the system engineering of his seismic experiment. One of the basic requirements of system engineering is to identify the function, in this case the delayed arming function, and then you consider all alternate methods of accomplishing it and then select the one particular method. For many years in the naval mine business the delayed arming has been a required feature of the naval mines and I'm sure the same in many types of fuses. The question is, what are the alternate methods of delayed arming that were considered and did the safety aspects of each alternate enter into the decision to choose the hair-springer method of delayed arming.

J. JONES: Primarily the alternate approaches that we had were a series of other kinds of timers or the use of more than one transmitter. There is one transmitter in the system now. I didn't take the time to explain that but there are three functions that must occur in order to get it to firing. Each of the two timers must operate and they must operate within certain time constraints relative to each other, and finally a signal must be received from the central station. An obvious approach, and it would have been terribly heavy in terms of weight, would be to use three transmitters which would mean three receivers in each package. There are eight packages so any weight penalty in the package is times eight. Still, from a safety viewpoint, we didn't like that because there are too many ways of generating spurious signals. The other alternate we had were other kinds of timing devices such as a tuning fork type watch or corts crystal regulated watch or using mission time and picking that up some how. All these fell by the wayside either because they were heavier or, in our opinion, less safe. What we selected we fell is the best, if we can make it work, and we are confident now that it will work.

QUESTION: I was very curious about the cause of temperature effect. Is the hair spring temperature dependent or not?

MR. JONES: It is not defined. Our watchmaking consultants are scratching their heads. There are several theories. The most viable one right now probably has to do with surface tension of the lubricant. Something else that I couldn't possible stuff into a half-hour presentation is that the lubrication problems are extremely difficult and that in itself is a two-hour presentation.

QUESTION: You have an oil type lubricant on a jewel bearing. I thought jewel bearings ran oil-free.

MR. JONES: No, all small watch mechanisms such as this do have wet lubrication. The particular lubricant that we are using costs about $10,000 a gallon and reliability is going nuts trying to get tracability all the way back to Switzerland on it. It is good, it works, and we are really quite surprised at the results of our temperature tests.

SESSION VI

SYSTEM SAFETY, THE CONSUMER, AND GENERAL INDUSTRY

Session Chairman - Dr. Leslie W. Ball

"Fault Tree Applications within the Safety Program of Idaho Nuclear Cooperation"	Dr. W. E. Vesely
"Consumer Product Safety - A Systems Problem"	Dr. Carl C. Clark
"Application of System Safety to Rail Transit Systems"	Mr. Thomas DeW. Styles
"Designing for Auto Safety"	Mr. Elwood T. Driver
"Integrating a Multifaceted System Safety Program for a Large Complex System"	Mr. S. W. Malasky
"Reliability Techniques in the Petroleum Industry"	Mr. Henry L. Williams
"System Safety Engineering in the Development of Advanced Surface Transportation Vehicles"	Mr. Harry E. Arnzen

N72-25981

FAULT TREE APPLICATIONS WITHIN THE SAFETY PROGRAM OF IDAHO NUCLEAR CORPORATION

By

Dr. W. E. Vesely
Senior Technical Specialist
Computer Science Branch
Idaho Nuclear Corporation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1 '1

INTRODUCTION

At Idaho Nuclear*, a system safety analysis program is in existence for the routine safety and reliability analysis of control and safeguard (backup) systems. Though the systems analyzed are generally peculiar to the reactor industry, the methods employed, and their applications, are generally utilizable in any safety program. In Idaho Nuclear's safety program, a diverse assortment of techniques are employed, such as fault hazard analysis, failure mode analysis (FMEA and FMECA), failure matrix methods, block diagram modeling, and fault tree methods. The fault tree method and its applications in particular are discussed in this paper, since this technique enters into a large portion of the safety analysis performed at Idaho Nuclear.

Fault tree methods are used to obtain both qualitative and quantitative information about the safety and reliability of the system analyzed. For the analysis, the fault tree depicts all the primary causes for a particular system failure (or accident occurrence). The system failure or accident occurrence is the top event of the fault tree. The primary causes are usually component failures, administrative errors or environmental conditions; in general, the primary causes depict the resolution desired for the causes of the system failure or accident occurrence. By use of the standard "AND" gate and "OR" gate symbology, the fault tree depicts the logical relationships of the primary causes, and their consequences, which led to the specified system failure (or accident). Figure 1 at the end of this paper summarizes the basic fault tree representations. For a discussion of the fault tree method, the reader is referred to Haasl(1) or Crosetti(2).

At Idaho Nuclear the fault tree analyses are performed for the following objectives:

1. To represent in an objective and communicative manner the causes of the system failure or accident occurrence.
2. To obtain the modes by which the system failure or accident occurs. These modes are termed "critical paths" in fault tree terminology.
3. To determine the relative importances of the individual critical paths.
4. To determine the qualitative and quantitative impact on safety or reliability due to proposed design modification or component upgrade.
5. To determine the quantitative response of system availability with regard to particular maintenance schemes.
6. To determine the quantitative safety, reliability, or availability with which to compare to established standards.

The fault tree itself satisfies the first objective since it portrays in a lucid manner the logical chains of events which lead to the system failure or accident. The fault tree, once drawn, is an effective implement by which management, reliability or safety engineer, and design engineer can communicate.

From the fault tree, a simple qualitative-type evaluation determines all the modes, or critical paths, for the system failure or accident. A critical path is a group of primary causes which must all occur in order for the system failure or accident to occur; if one of these primary causes does not occur then the system failure or accident will not occur by this mode. The complete set of critical paths for the fault tree gives all the combinations of primary causes which give rise to the top event. If one or more of these combinations occurs, then the system failure (or accident) occurs.

A few simple illustrations may serve to best clarify the critical path definition. Assume a fault tree has been drawn and its critical paths have been obtained. If one of these critical paths is "Resistor 1 Failure in Mode A" and "Resistor 2 Failure in Mode B" then Resistor 1 must fail in Mode A and Resistor 2 must fail in Mode B in order for the system failure or accident to occur. If either resistor does not fail, or fails in modes other than A and B, then the top event (system failure or accident) will not occur by this particular route. If one of the critical paths obtained is "Resistor 3 in Mode A", then only Resistor 3 failing in Mode A is sufficient for the top event to occur, and Resistor 3 in

* As of July 1, 1971, Idaho Nuclear will be under the Aerojet Management and will be known as Aerojet Nuclear Company.

Mode A" is termed a single failure. The set of critical paths obtained for this fault tree represent all those primary cause combinations, and only those combinations, which will cause the top event to occur.

The critical paths are obtained from the fault tree by means of a number of existing safety and reliability computer programs; at Idaho Nuclear the programs PREP and KITT(3) are used. The critical paths are an important class of information since they directly tie the system failure or accident to the primary causes. If improvement is desired, the critical paths identify the specific areas which are the weakest and which would have greatest response to an improvement. In general, optimal improvement consists of increasing the size of the smallest critical paths. If the fault tree has one component critical paths (single failures) improvement should be centered such that these paths become two component (a redundancy added), if two component critical paths are the smallest that exist for the fault tree, then they should be designed into three component critical paths and so forth.

For the quantitative information in the preceding list of objectives of the fault tree analysis, the computer programs PREP and KITT are utilized. PREP and KITT employ the Kinetic Tree Theory approach to obtain quantitative information about the fault tree. The Kinetic Tree Theory technique has been described in a number of articles (4,5,6) and the details of this approach will not be discussed here.

The fault tree as drawn by the engineer is simply input into PREP and KITT. The only other data needed as input are the failure rates or probabilities for the primary causes (i.e., for the components and any environmental effects) and the average repair times for those primary causes that are repairable. With this input data, PREP and KITT obtain the critical paths of the fault tree and the following quantitative information:

1. The probability that the failure or accident will not occur at all to time t.
2. The probability of the failure or accident existing at time t.
3. The expected number of times the failure or accident will occur to time t.
4. The failure or accident frequency at time t (the integral of this quantity is simply the previous characteristic (3)).
5. The failure rate (lambda) at time t.

This information is obtained for any series of time points t desired by the user, and hence time dependent curves are obtained which portray the time history of the reliability or safety. From these curves one is able to discern, for example, the degradation of reliability or safety with respect to time; lifetime-type information is thus included in the results obtained. If a particular time is of interest, then one point from these curves is simply used.

This time dependent information is obtained for each primary cause of the fault tree (i.e., for each component or environment effect), for each critical path of the fault tree, and for the top event of the fault tree (the accident or system failure of interest). As applied to a particular primary cause, the information gives the frequency at which the primary cause occurs, the probability of the primary cause not occurring at all, the probability of the primary cause existing at time t, and the expected number of times the particular primary cause will occur. If the primary cause is a component, the information thus gives the detailed reliability and availability of the component and shows, for example, the detailed effects of repair or environment stresses on that particular component. Since this information is obtained for every primary cause, those primary causes, such as particular component failures or environment effects, which are most critical are readily identified.

The information obtained for a particular critical path gives the frequency, expected number of times, etc., the top event (i.e., system failure or accident) will occur by this particular mode. The primary causes in the particular critical path are solely responsible for the system failure or accident and the obtained information describes how often this particular critical path, or mode, will cause the failure or accident. The information is obtained for each of the critical paths of the fault tree, and hence the most important critical paths are identified, those by which the failure or accident will most likely occur.

Any safety or reliability improvements will be directed to these "weak links".

In addition to being obtained for each primary cause and critical path, the five time dependent characteristics are also finally obtained for the top event of the fault tree. The characteristics give the frequency at which the system failure or accident will occur, the number of times it is expected to occur, and the probability of it not occuring at all. If the system analyzed is a safety backup-type system, this information gives, for example, the availability of the system, that is, the probability that the system will perform correctly when an accident condition exists. For an on-line operating system, the information gives the percentage of time the system will operate without failure in any time period. The information obtained is a complete characterization of the failure or accident for any particular situation analyzed; effects of repair, environmental stress, and administrative procedures are explicitly obtained. Since the information is time dependent, a complete history of the safety and reliability characteristics is yielded.

The PREP and KITT codes obtain the time-dependent characteristics by an analytical technique which does not entail any Monte Carlo simulation. The codes require little computer time, for example, approximately two minutes of IBM 360/75 computer time is needed to completely analyze a 1000 component fault tree. For smaller trees the computer time is considerably less*. Because of the small computer time, sensitivity studies and design modification studies are practically performed. The failure rates, repair times, or particular portions of the tree are simply modified and the programs run again to assess these possible deviations.

PARTICULAR APPLICATIONS

This section describes particular fault tree analyses which have been performed at Idaho Nuclear. The specific, technical details of the systems are not described so that the reader is not encumbered with jargon with which he may not be familiar. The aim of this section is to demonstrate, as straightforwardly as possible, practical applications of fault tree analyses. By describing the results which have been obtained from these analyses, this section will hopefully illustrate the power of fault tree analysis and the role it can play in a system safety program.

SPERT IV Protection System Analysis*

The SPERT protection system is an electrical control system which has the function of shutting the reactor down when certain safety criteria are exceeded. In this particular instance, the system consisted of an automatic control (time triggered) and a manual backup control. If the automatic control system failed, a signal was relayed to an operating personnel who was then to initiate the manual control system (by pressing a control button).

A fault tree was drawn for this system, in which the system failure (top event) was defined to be both the automatic control system failing and the backup manual control system failing, when accident conditions existed. In this case, an analysis was performed on an already existing system; the SPERT control system (automatic and backup) was operating, but an upgrade was desired. In order to upgrade this system, the following information had to be obtained:

1. An identification of all credible component failures and/or fault conditions that could result in the designated system failure.
2. An identification of the most critical weaknesses in the existing system (termed the "base-line" system).
3. A determination of the impact on system safety due to proposed design modifications.

The fault tree was decided upon as the most practical method of obtaining this information. The fault tree analysis was performed independently of other safety analyses and was the major effort for this particular system study.

The fault tree, once it was drawn, consisted of approximately 300 component failures

*The computer time is insensitive to the number of time points desired by the user.

*SPERT IV is the name of a particular reactor.

and fault conditions (primary causes). The primary causes (the "bottom ends" of the fault tree) were basic component failures such as particular resistor failures, relay failures, and wire failures. Adverse environmental conditions on these components were also included in the primary causes. The resolution of the fault tree was therefore on a basic component level.

A correct input to the automatic and backup control systems was assumed and the fault tree analyzed the causes for no output or incorrect output. Hence, the analysis isolated the "signal-passing function" of the control system. No human errors were considered in the fault tree. Certain subsystems of the control system were periodically checked and this scheduled maintenance was included in the analysis. To draw this fault tree, a total time of approximately two man-weeks was required. This task thus required little time and effort.

The fault tree itself and the critical paths determined by PREP and KITT yielded the first class of information in the preceding list. In the PREP and KITT computer run, failure rates (lambdas) were assigned to the components on the fault tree to determine the most import critical paths, i.e., to identify the most severe weaknesses in the system. The results of this run are shown below.

Table 1

COMPONENT FAILURE CONTRIBUTIONS TO A SYSTEM FAILURE

Manual Control Failure

Component	Failure Contribution
Relays (8)	0.6477
Console Switches (2)	0.3076
Terminals and Connectors (27)	0.0262
Wires (76)	0.0185

Automatic Control Failure

Component	Failure Cont. ibution
Timer (1)	0.9927
Relays (14)	0.0071
Terminals and Connectors (26)	0.0001
Wires (71)	0.0001

The above table lists only the major contributors to system failure; the numerous other components not listed had negligible contribution. From the table, if the automatic control system failed, 99% of the time it would be due to the automatic timer mechanism itself failing, while only 0.01% of the time it would be due to one of or more of the 76 wires failing. If the manual backup system failed, 65% of the time it would be caused by one or more of the eight relays failing and 31% of the time would be caused by one or both of the console switches failing. The critical area in the automatic system was thus the timer mechanism while the critical areas in the manual backup system were the eight relays and two console switches.

From the identification of these critical areas, and from the critical paths and fault tree itself, which showed the interconnections these critical areas had within the system, modifications become evident which might upgrade the safety of the system. The modifications were quite simple and consisted of 1) placing a second relay in parallel with an existing one ("Modification 1"), and 2) inserting a manually set timer in the automatic control circuit ("Modification 2"). The impacts of these modifications were determined by two additional PREP and KITT computer runs which analyzed the fault tree with the modifications inserted. The total IBM 360/75 computer time required for these two runs plus the original run was three minutes, which was neglible. The result of the impact evaluations is shown in Figure 2 at the end of this paper.

In the figure, the "Failure Probability" is that both the automatic control system and the manual control system will fail in any one or more of the number of tests performed (a "test" here is simply an operation of the control system). For example, the failure probability at 200 tests denotes the probability of control failure in one or more of these 200 tests. The "BASE-LINE" curve depicts the failure probability for the existing automatic and backup system, the "MOD-1" curve is for this system incorporating Modification 1 (described previously), and the "MOD-2" curve is for the system incorporating both Modification 1 and Modification 2.

As evident from the figure, the proposed modifications significantly increased the safety of the control system. These modifications were made evident from the fault tree analysis and the impacts of these modifications were then able to be objectively determined from the PREP and KITT computer runs. Modification 1 (corresponding to the MOD-1 curve) was consequently decided upon as a change to be incorporated in the system which would be practical in cost and which would substantially upgrade system safety.

Plant Protection System Pilot Study

The system analyzed in this study is an on-line control system. Critical plant parameters are continuously monitored and if any of these parameters exceeds safe operating limits the control system rapidly reduces the reactor power. The fault tree analysis was performed during the conceptual phases of system development. Three possible designs were proposed for the control system, and the fault tree analysis served the role of determining the "best" system design out of the three proposed. The analysis investigated both the safety and reliability of the designs; in fact, in this instance, if the system safety was the only characteristic examined the wrong design would have been chosen.

The fault tree analysis of the three designs was conducted on a functional level; the minimum components required to provide a discrete and separate function were considered as the basic building blocks of the system. This level of analysis was sufficient to define the primary causes of failure on the fault tree. Any further detail was inappropriate in this conceptual design phase and the functional level of resolution provided adequate information with a minimal expenditure of time and effort.

Six fault trees were drawn for the three proposed designs, one fault tree considering reliability and one fault tree considering safety for each design. The studies were performed by system design engineers who were familiar with the concepts of fault tree analysis. Each fault tree consisted of approximately 70 components (primary causes) and the six fault trees required two man-weeks to complete (two engineers working five days).

Each of the three designs possessed redundancies in the electrical circuits. All the designs utilized two out of three coincidences to insure against spurious, undesired action, and all three designs were of the same order of cost. It was not obvious from the design as to which one design was the best and a fault tree analysis was the only method deemed practical, and of sufficient power, to solve this problem.

For the safety fault tree of each design, the system failure (top event of the tree) was defined to be "failure of the system to respond when protective action is necessary". For the reliability fault tree the system failure was defined as "system responds when protective action is not necessary". For the safety study the failure thus investigated was the system not working when accident conditions existed; accident conditions were input to the system, but the system did not respond. For the reliability study, the failure was the system acting as if accident conditions existed when they did not; normal, nonaccident conditions were input to the system, but the system responded as if accident conditions were input. In the safety failure, the system gave no protection to an accident and in the reliability failure, the system gave unwanted protection which shut the plant down.

The fault trees, once drawn, were input to the PREP and KITT programs to obtain the quantitative system safety and reliability characteristics. Component failure rate data, gathered from existing reports, was also input to the programs. The same failure rate data was used for all the fault trees in order to obtain valid comparisons. The six computer

runs required a total of four minutes computer time, which was inconsequential. The results of the analyses are shown in Figures 3 and 4 at the end of this paper.

In Figure 3, the probability of a safety failure is plotted versus total operating time (hours). A point on a curve gives the probability of the system failing during a particular operating period. If, for example, the time period of 1200 hours is chosen (the x value) then the probability that the system will fail during this 1200 hour operating period is obtained from the curves. (The curves in Figure 3 are only plotted to 2000 hours since this is the proposed maximum continuous operation time for the system.)

The system failure investigated in Figure 3 is a safety failure, i.e., the failure of the system to respond when protective action is necessary. Each of the three safety fault trees for the three designs investigated this particular safety failure (had this as the top, undesired event on the fault tree). "System I", "System II" and "System III" in Figure 3 represent the three individual design proposals. From the figure, System I and II are the safest designs with System II being a bit safer than System I. If safety was the only consideration, then System II would be chosen as the best design since it was simpler and slightly cheaper than System I.

Figure 4 illustrates the reliability of each of the three designs. The probability of a reliability failure (the y-axis) is the probability that the system responds when protective action is not necessary. Total operating time is again depicted on the x-axis. From the figure, System I is the most reliable, while Systems II and III are highly unreliable and cause numerous unwarranted shutdowns.

Investigating both Figures 3 and 4, that is investigating both safety and reliability, System I is clearly the best design. The safety of System I is acceptable with regard to the established program standards and in fact the difference between the safety of System I and the safest design is insignificant. The reliability of System I equals its safety ($\sim 10^{-3}$ after 2000 hours) and far exceeds the reliability of the other two designs. Because of this analysis, System I was the design chosen and is presently progressing through the finalized design stages.

For this study, the fault tree analysis thus allowed the best design to be chosen with little effort and cost expenditure. System III was the simplest design and had the fewest components, while System I, the design chosen as the best, was the most complex. The fault tree analysis showed that in this case, a small amount of added complexity bought large returns in safety and reliability. As an added verification, the present finalized design studies of System I substantiates completely the results of the performed fault tree analyses.

PBF Poison Injection System Analysis

The final study discussed in this paper is an investigation of a backup emergency system. The poison injection system is used as an emergency reactor shutdown system; it is essentially a two out of three type control system which is manually initiated. A correct input to the system was assumed and no response was the system failure examined (i.e., this was the top event of the fault tree). Resolution was on a basic component level and human errors were not considered. The fault tree analysis was performed again during the conceptual design stage. The fault tree consisted of approximately 200 components and, as in the previous cases, required approximately two man-weeks to complete.

The analysis is different from the previous two in that the injection system is solely a backup system and system availability is the primary safety concern. ("Availability" here is the probability the system will function when called upon at any particular time. Conversely, the "unavailability" is the probability the system will not function when called upon.) The fault tree analysis was performed to investigate the following:

1. Possible weaknesses in the system design (the base-line system). These would be determined from the fault tree itself and from the critical paths obtained by PREP and KITT.
2. The response of system availability with regard to various maintenance checking intervals used for the components. This would be determined from the quantitative characteristics obtained by PREP and KITT.

3. Differences that would result in system availability due to particular design modifications. The quantitative characteristics from PREP and KITT would again be used here.

The fault tree analysis was one part of a larger safety analysis performed on this system.

The fault tree, having been drawn for the base-line system design was input to the PREP and KITT codes to obtain the critical paths and quantitative characteristics. The input also included the component failure rates and a range of checking times for those components that would have maintenance (not all components would be checked and this was taken into consideration). From the fault tree and critical paths, possible weaknesses in the base-line system were uncovered. A second and third computer run was then performed to analyze two possible design modifications; in these additional runs, the same component failure rates and checking times were used. The total computer time required for the three runs was five minutes IBM 360/75 time.

Figure 5 at the end of the paper shows the system availability versus component checking interval for the base-line system design and for the two proposed design modifications. The quantity actually plotted on the y-axis is the failed probability, or system unavailability, which is one minus the availability. The "NO REDUNDANCY" curve is the based-line system, the "PARTIALLY REDUNDANT" curve is for a design modification making certain portions of the system redundant, and the "COMPLETELY REDUNDANT" curve is for a second design modification making the system completely redundant.

From the figure, for example, if the maintainable components of the base-line system were checked every 100 hours (10^2 on the x-axis) then the system unavailability would be 6×10^{-2} (the corresponding y-value on the NO REDUNDANCY curve). Thus, for this design and checking interval, 6% of the time the system would not function when called upon.* Again, for the base-line system, if the maintainable components were checked every 1000 hours, then the system unavailability would be 4×10^{-1}, i.e., there is a 40% probability that the system would not function when it was called upon at any particular time, (when accident conditions existed). The unavailability for the PARTIALLY REDUNDANT design or the COMPLETELY REDUNDANT design, for a particular component checking interval, would be read from the figure in a similar manner as above.

The results from the fault tree analysis and the subsequent PREP and KITT runs shown in Figure 5 are significant since they show not only the response of availability with respect to various maintenance schedules for a particular design, but also show the impact of design modifications on the system availability. If a given availability is desired (or equivalently if a given failed probability, or unavailability, is desired), then either the base-line system design with a given component checking interval may be used or a modified design with a larger checking interval may be used. The design modifications have their chief impact on the checking interval, allowing the same availability to be attained with less maintenance.

The modifications which made the system completely redundant (the COMPLETELY REDUNDANT curve in Figure 5) consisted of incorporating more piping redundancy into the system. These modifications increased the independence of the flow circuits as verified in Figure 5. The modifications have been taken into consideration in the final design of the system.

Finally, Figure 6 shows the failed probability (unavailability) for the completely redundant design when possible errors in component failure rate data are taken into account. The "MOST PROBABLE VALUE" curve in Figure 6 is the same as the COMPLETELY REDUNDANT curve in Figure 5, but is plotted on a different scale. The MOST PROBABLE VALUE curve represents the best value for the completely redundant system unavailability. The "90% Upper Bound" and "90% Lower Bound" are the 90% confidence bounds for the system unavailability (i.e., the curves represent 90% error bars when possible errors in data are taken into account). These upper and lower bound curves were computed by

*Checking every 100 hours means a periodic maintenance check is performed after every 100 hours of operation.

assuming a possible error of a factor of 10 in each component failure rate (to 90% confidence). These error curves serve to show the effect errors in component failure rate data have on the system computed safety characteristics. As observed, the possible errors did not significantly affect the system results. Even accounting for these possible component failure rate errors, the relative differences between the curves in Figure 5 remained the same (i.e., the possible failure rate errors merely shift all the curves in Figure 5 up or down the y-axis without changing their relative separations). The completely redundant system thus still showed the same gain in availability when possible errors in component data were taken into account.

For this study of a stand-by emergency system, the fault tree analysis thus showed, in an objective manner, the effect of maintenance on the system availability and the effect of proposed design modifications on the availability. As for the previous studies, the fault tree effort required minimal time and cost, with returns greatly exceeding the investment.

SUMMARY

The fault tree methods that were used for the described analyses are not peculiar to any particular system; the methods can be used on any electrical or mechanical system in any industry. Furthermore, the methods need not only be applied to systems, but can be applied to any event or incident, such as an accident occurrence, for which the primary causes are desired. The same kinds of results as were illustrated in this paper will be obtained for any fault tree, regardless of its particular nature. Any fault tree will yield, among other information, the critical paths, i.e., the modes by which the system failure or accident will occur, the most critical areas likely to cause the failure or accident, detailed failure probabilities, and the response of safety or reliability to design modifications and maintenance schemes. The fault tree itself is a significant result since it objectively defines the failure or accident and is valuable tool for communication. The fault tree analysis has most application in the design phases, but it can be used on already existing systems. Finally, the fault tree can be as detailed as desired, however, the fault tree need not be elaborately complex in order to yield useful and significant information.

REFERENCES

(1) D. F. Haasl, "Advanced Concepts in Fault Tree Analysis", System Safety Symposium, June 8-9, 1965, Seattle: The Boeing Company, 1965

(2) P. Crosetti, "Fault Tree Analysis with Probability Evaluation", in IEEE Transactions on Nuclear Science, Vol. NS-18, (1), February, 1971

(3) W. E. Vesely and R. E. Narum, PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree, IN-1349, August, 1970

(4) W. E. Vesely, "Reliability and Fault Tree Applications at the NRTS", in IEEE Transactions on Nuclear Science, Vol. NS-18, (1), February, 1971

(5) W. E. Vesely, "A Time Dependent Methodology for Fault Tree Evaluation", Nuclear Engineering and Design, 13 (1970) pp. 337-360

(6) R. E. Narum, "A Rapid and Exact Methodology for Fault Tree Analysis", Proceedings of the Semiannual AEC Computer Information Meeting, 1969

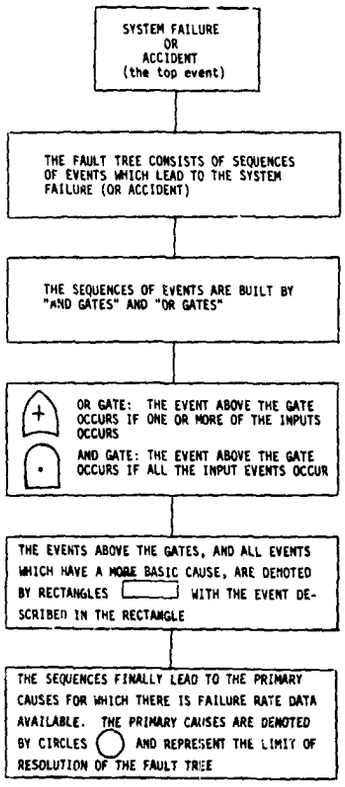


FIGURE 1

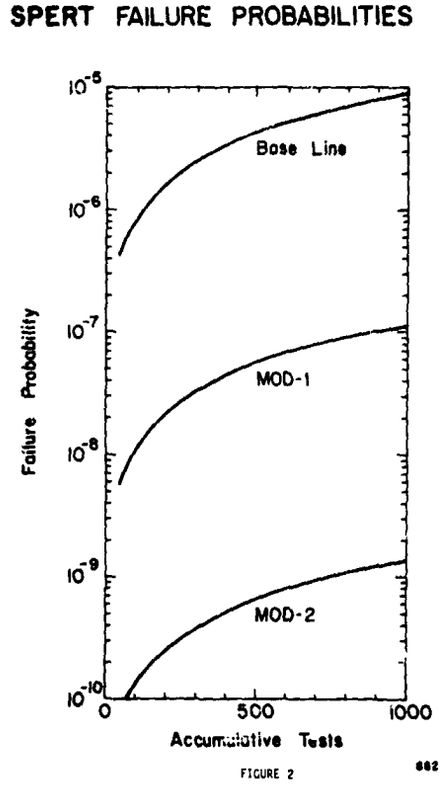


FIGURE 2

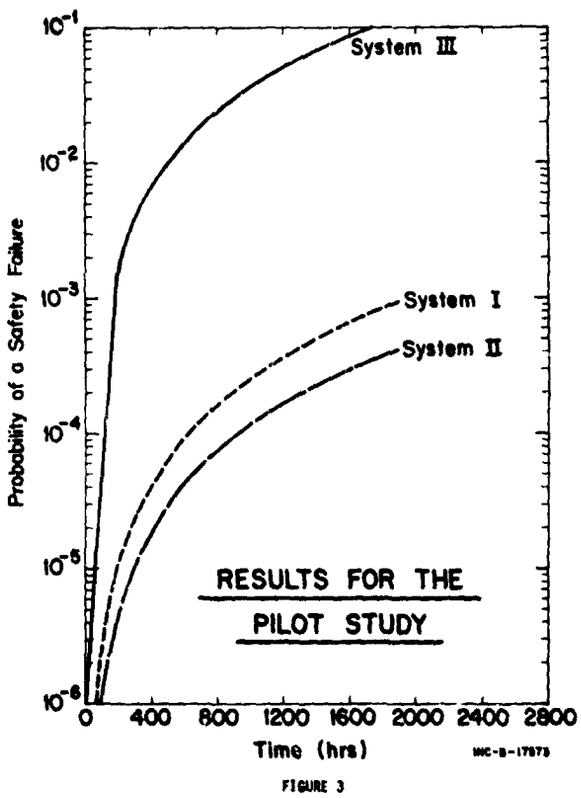


FIGURE 3

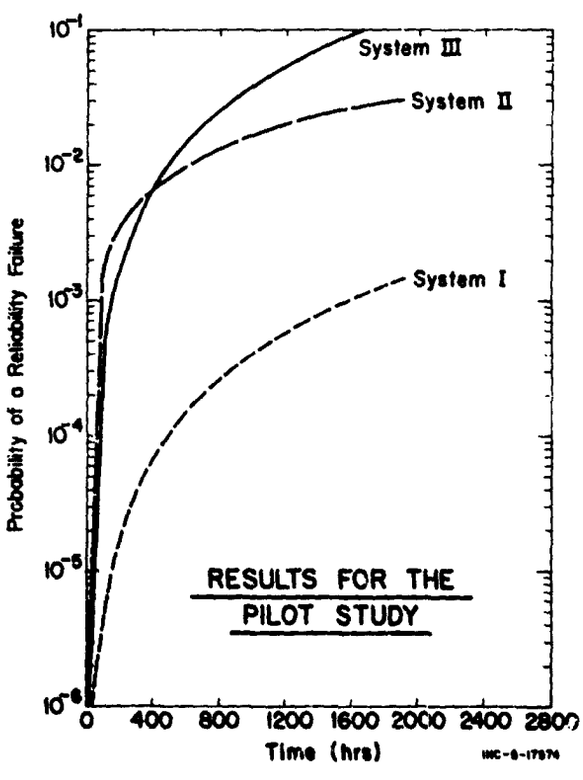


FIGURE 4

FAILED STATE PROBABILITY
VERSUS CHECKING INTERVAL

(relative to design)

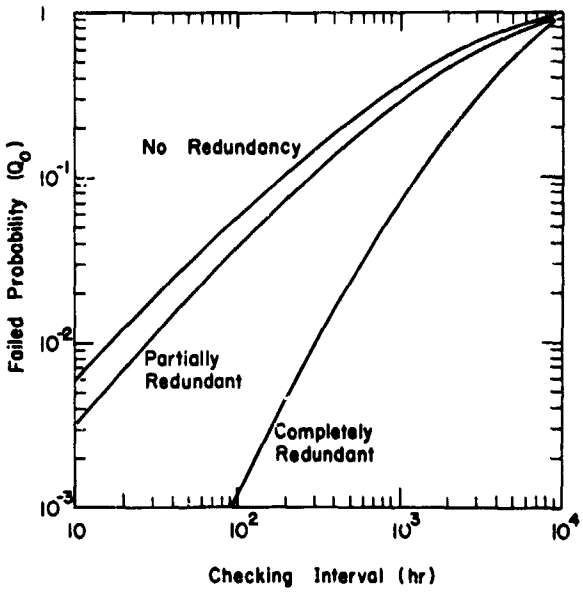


FIGURE 5

INJECTION FAILED STATE PROBABILITY
VERSUS COMPONENT CHECKING
INTERVAL

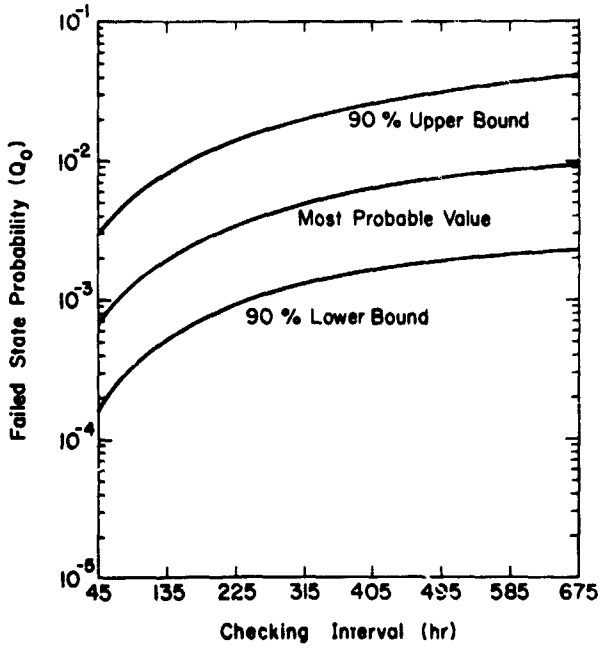


FIGURE 6

N72-25982

CONSUMER PRODUCT SAFETY

A SYSTEMS PROBLEM

By

Dr. Carl C. Clark
Staff Consultant
on
Product Safety

National Bureau of Standards

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

CONSUMER PRODUCT SAFETY--A SYSTEMS PROBLEM

by

Carl C. Clark
Staff Consultant on Product Safety
Product Evaluation Technology Division
National Bureau of Standards
Washington, D.C. 20234
301-921-2967

for presentation at the

Government-Industry System Safety Conference

sponsored by the

National Aeronautics and Space Administration
Goddard Space Flight Center
Greenbelt, Maryland

May 26-28, 1971

ABSTRACT

The manufacturer, tester, retailer, consumer, repairer disposer, trade and professional associations, national and international standards bodies, and governments in several roles are all involved in consumer product safety. A preliminary analysis, drawing on system safety techniques, will be utilized to distinguish the inter-relations of these many groups and the responsibilities that they are or could take for product safety, including the "slow accident" hazards as well as the more commonly discussed "fast accident" hazards. The importance of interactive computer-aided information flow among these groups will be particularly stressed.

NBS Document 411.00 CM035 - Revised

This document represents the views of the author, but not necessarily those of the National Bureau of Standards administration.

INTRODUCTION

The simplistic pictures of life's problems confound efforts to deal with the solutions, in their intricate complexities. Some of us may be attracted to the slogan solutions - "accidents are caused by the nut behind the wheel" - but study soon shows that human events, such as an injury while using a consumer product, cannot be said to have one cause, one fault, one solution. It obscures understanding and yields limited improvement to look for and try to act on the cause of an accident. [illegible] events have thousands of "causes" or antecedent events, many of which might be modified to increase safety.

This is "coal to Newc[illegible] system" safety engineers in their own specialties - particularly space safety or military systems safety. But we are just learning to apply these techniques to consumer product safety. How many aerospace systems safety engineers apply these techniques in their own homes? Instead of waling junior right away for leaving books on the stairs that pa tripped over, how many of us analyse the many changes that would have reduced the chances of this event - improved lighting, wider stairs, tables near the bottom and top of the stairs for holding things we wish to later take up or down, less to drink before dinner, less shouting at the family and stomping on the stairs to show who's boss, etc. - before waling junior?

Clearly, the systems effectiveness and systems safety techniques of analyses of reliability, maintainability, operability, supportability (logistics), compatibility, design simplicity, human factors, dependability, availability, hazards, failures, fault trees, environment effects, systems safety plans, safety documentation and communication, safety audit procedures, etc., could be utilized to increase the safety of consumer products and their use.

For space and military products, the government has the responsibility and the capability through contract requirements and payments to minimize the costs of product purchase and product use, including the human and dollar costs of safety failures. For consumer products, the picture is less clear as to who is responsible for safety, and the capabilities of the individual product purchaser, the consumer, are far less than the government to specify or even to find out the level of safety or other use costs of the products he buys. The cost of safety features is localized with the price of the product; the savings of safety are very distributed. But consumers, acting as voters, are expressing a group interest through legislation for more government concern with increasing the safety of consumer products.

THE SAFETY INTERFACES

Figure 1 diagrams some of the more important safety interfaces. Traditionally, the consumer exchanges money with the manufacturer for products, and has the responsibility (caveat emptor - buyer beware) to select the products that serve his needs, using injuries as experience in judging safety. As the market has proliferated so that experience with particular products is more diffuse, and as products have become more complex, so that their hazards are largely hidden, governments, particularly through judicial powers and tort law development, have held the manufacturer increasingly responsible for his product (caveat vendor - seller beware). As Morris Kaplan put it, (1)

> "The consumer has a lot of catching up to do. Much has happened between the hoe and the mechanical cultivator, between homespun and polyester knits, between illustrated books and color television. By the time he learns about a gas or electric stove, there's a radar oven. After he learns the difference between real and artificial silk, he is confronted with acetate, nylon, polyester, acrylics."

The manufacturer gives an implied warranty for his product, and may give an express warranty as well, but it is noted that his responsibility for his product is far from complete. His express warranty may cover only a few percent of the design use life of the product, and products liability insurance and case settlement payments of 0.05% of sales are not unusual. (2)

Looking again at Figure 1, it is the government far more than the individual consumer that has utilized injury information. Through legislation and regulation (or executive law), the government requires the manufacturer to consider certain aspects of consumer product

safety (cave legem - beware of the law, an expression I suggest). However, the government has had only a moderate impact on consumer product safety in any given decade - although the combined effects are very important, and total hazards perhaps particularly in food and drugs might be far worse without any government action. Hence, the practice of the marketplace continues to be caveat emptor - buyer beware - however much we talk about products liability, class action, self-regulation, and government regulation trends.

It is the consumer who pays - is handed the responsibility - for most (I suggest about 90%) (3) of the product performance failures, and most (I suggest 50%) of the costs of injuries involving the products he buys. (My rough working estimate (3) is that the manufacturer pays through products liability settlements perhaps 5% of the injury costs of consumer products, i.e., that only 5% of the injury costs show up directly in product prices. Governments, through support of the medical establishment, pay some 30% of product injury costs, I estimate - which show up later in taxes. And uninjured consumers, through insurance distribution, pay perhaps 15% of product injury costs.)

The importance of the testing laboratories and standards bodies in consumer product safety is now growing.

SLOW ACCIDENTS

In addition to our dollar losses for unwise choices in the marketplace, we have our human losses of deaths and injuries while using products. The National Safety Council Accident Facts reports some 115,000 accident deaths and 50 million injuries per year, of the 2 million who die each year in the United States. I call these the "fast accidents," and am looking particularly at the deaths and injuries involving delayed stress effects of our life styles, the "slow accidents" (3) of carcinogens in our products and environments, heavy metals in our streams, deaths and hospitalization (injury) for some people with "diseases" including malnutrition whose cures or prevention are known but not applied, and all other effects of stress that lead to "premature death" and hospitalization. Ralph Nader speaks of the "silent violence" of our society. By a curve fitting procedure, Figure 2, of the cumulative percent of those who died in 1967 (4) versus the age at which they died, the preliminary suggestion is made that the observed curve could be accounted for by a "biological death" probability distribution with mean age of death of 75 and standard deviation of 12 years, with a 2 percent "tail" of additional deaths prior to the age of 1 year representing the early-lethal effects, together making up 70 percent of the deaths, and a difference curve "stress death," which is within 4.5 percent of being a straight line -- with less deaths before age 50 and more after age 50, curve fitting at 30 percent of the deaths--or 600,000 people per year in the United States.

On the basis of this very preliminary hypothesis, I suggest that in addition to some 100,000 fast accident deaths there are some 500,000 slow accident deaths, and with an estimated ratio of perhaps 500 injuries to 1 death, there are 250 million slow accident injuries per year -- to the extent of getting professional medical treatment or being disrupted from normal activities for at least a full day. Most of us are feeling some discomfort with our technological life style -- although I hasten to emphasize that it is this same technology that lets many more of us live out a biological life span than in years past. The median age of death in Massachusetts in 1850 was 40, and even in 1900 for non-whites it was 33. (4)

The challenge in consumer product safety, then, is not only to reduce at least the involuntary imminent hazard aspects of product use, but also to reduce these continuing hazards of pollution, mutation, exhaustion of raw materials, and other stresses of modern life. By increasing production of food, products, and services over the millennia man has indeed extended the median life span. Now, in this generation, it becomes apparent that much further increased production and populations will decrease the median life span unless we reduce the stress hazards. Living with man rather than living with nature has become the challenge of survival.

INFORMATION VERSUS REGULATION

As Figure 1 indicates, there are several ways in which product injury information could

be more effectively utilized in the marketplace. The government staff could decide what is needed to increase safety and by legislation and regulation require that these changes be made. Many of us are aware of the inadequacies (6) of bureaucratic omniscience, and feel that regulation should deal with only the unreasonably hazardous products.

A major alternative to encourage the use of safe and well-performing products, i.e., products with reduced imminent or delayed hazards, is for the government and the manufacturer to increase the flow of product information to the consumer, to increase his ability to choose safety. We often get the wrong product or the wrong service -- not the one we would have chosen even with our present education if we had been given adequate information about products and services in the marketplace. President Nixon, in his Consumer Message to Congress (7) of February 24, 1971, after noting the major success of our economy, said,

> "In today's marketplace, however, the consumer often finds himself confronted with what seems an impenetrable complexity in many of our consumer goods, in the advertising claims that surround them, the merchandising methods that purvey them and the means available to conceal their quality. The result is a degree of confusion that often confounds the unwary, and too easily can be made to favor the unscrupulous. I believe new safeguards are needed, both to protect the consumer and to reward the responsible businessman."

The President then presented legislation to implement the "buyer's bill of rights," including the right to information to make intelligent choices among products and services in the marketplace, and concluded;

> "In submitting the foregoing proposals, I want to emphasize that the purpose of this program is not to provide the consumer with something to which he is not presently entitled; it is rather to assure that he receives what he is, in every way, fully entitled to. The continuing success of our free enterprise system depends in large measure upon the mutual trust and goodwill of those who consume and those who produce or provide.
>
> "Today in America, there is a general sense of trust and goodwill toward the world of business. Those who violate that trust and abuse that goodwill do damage to the free enterprise system. Thus, it is not only to protect consumers, but also to protect that system and the honest men who have created and who maintain it that I urge the prompt passage of this legislation program."

What then is the buyer's right to information about products to allow intelligent choices in the marketplace? I shall present a preliminary and personal view here, with the emphasis that it would be a great service of the engineering community and of this conference to refine this list and begin to implement its use.

My view is that, just as one manufacturer would require the following from another manufacturer supplying a product, so the consumer has a right to know

- the name and address of the manufacturer. If the manufacturer is outside of the United States, the name and address of the importer should also be given
- the model number, and perhaps for products costing over $100 a serial number of the product
- the date of manufacture
- the design performance under design use conditions
- the design maintenance under design use conditions, and costs
- the design repairs: characteristics, costs, and frequencies under design use conditions
- the design use life under design use conditions
- the standards and test methods followed in design and manufacture
- the quality control utilized. Test methods, frequency of use, results for the design product, and accepted variations for all tested products sold.
- the kinds of accidents and their frequencies and severities for products of this category, and what has been done in this particular product to reduce these accidents
- the residual risks of accident types -- with predicted frequencies, severities, and costs -- for accidents which have

not been avoided by the product design. These residual risks must remain of user concern.

- warning and hazard instructions--how to recognize and avoid hazards, and what to do if hazards develop
- warranty, if offered, including time and procedures, and the percent of design product use life under design use conditions which is covered by the warranty
- how to get in touch with the manufacturer for complaints, repair advice, etc. Ideally a reverse-charges telephone number such as is being used by one large manufacturer
- user experience concerning performance, repair, problems, etc. as reported to the manufacturer or to the government, or as solicited by the manufacturer from a statistically balanced sample of users. Because of possible conflict of interest problems, this might better be presented as a summary of government complaint and use data rather than as manufacturer data.

The responsible manufacturer, in his design of a consumer product, already has most of this information, and could now put it in a Buyer's Handbook, available on request if not supplied with each product sold. But there is a lot of work to do by industry, by government, by standards bodies, and by all engineers to indeed make this information meaningful to the consumer, and used to reduce waste and hazard in the marketplace.

Dr. Lewis Branscomb, Director of the National Bureau of Standards, presented the buyer's right to information in the following form: (8)

"Information

The buyer needs the answer to three questions about a product:

1. How well will it do the job I want it to do, and for how long?
2. How much does it cost me, now and later?
3. Is it safe? Will it annoy my neighbors?"

The extent to which industry and government supply such information to consumers, so that short-term and long-term safety become factors in the marketplace, will in my view determine the extent that mandatory regulation of safety is considered unnecessary. I suggest the phrase "Cave Consumptorem Prudentem - beware the wise consumer". Either the consumer will be given the information that will let his wise choice in the market correct the unreasonable dangers and waste of incorrect choice, or in his growing political wisdom he will vote to remove these dangers and wastes by regulation. The responsible manufacturer has nothing to fear, and indeed in my view should speed the day of wise choice in the marketplace by preparing a Buyer's Handbook on each model of product sold, with all of the informatim listed above.

THE MANUFACTURER

In an altruistic world, the manufacturer would practice every known procedure to insure the short term and long term safety of the users of his product. But without altruistic stockholders, his need is to show a profit from his management. He may conclude that since he is only directly paying a small part of the cost of injuries and other failures involving his products, he may do less for safety, in keeping with his own financial realities (9). This condition may prevail until the costs of product failures are at least identified for the information of future buyers if not indeed charged back to the manufacturers.

The National Commission on Product Safety examined the safety practices of a small number of manufacturers of consumer products by means of a Manufacturers Questionnaire. Responses were voluntary, so perhaps better than average performance is practiced by those agreeing to respond. An index representing the percentage of yes responses concerning the performance of recognized systems safety practices was utilized to examine a number of industries (2). Figure 3 illustrates the spread of total responses, from the 20% for the footwear industry - whose questionnaires showed almost no sense of involvement with the problem that the major source of injury in the home is from falling - to the 88% for the power tool industry, who are well aware of tool hazards and attempting to reduce them. Reference 2 should be examined for the kinds of safety practices of certain consumer product industries.

Looking again at Figure 1, the manufacturer could investigate product injury problems directly, and use this information to improve his product. The National Commission on Product Safety found very few manufacturers who had physicians or related personnel visiting hospitals, medical researchers, and injured individuals to learn details of product injury events. Although manufacturer injury investigation personnel, with medical as well as engineering experience, would have difficulty finding appropriate cases to investigate working alone, the time is at hand for at least all large manufacturers to designate staff injury investigators or coordinators to cooperate with the Government in these studies. The patient privacy and investigator conflict of interest issues are important, so that the Government may do much of the initial investigation alone. But the manufacturer in my view should seek his own professional understanding of the public health product injury problem, and not wait for the Government to spell out for him the mandated engineering changes.

THE TESTER

To help assure the safety of a manufactured product one can test the product. "Hazardous or unsafe conditions for individuals using, maintaining, or depending upon the product" are considered "Critical defects" for products supplied to the Government, and "the supplier may be required to inspect every unit of the lot or batch for critical defects." (10)

The individual consumer can make no such 100% inspection requirement, but none the less the trend in consumer product testing is toward 100% production line testing. The cost of machine testing is going down in comparison to the cost of off-line "handcraft era" testing of the older quality control methods, and the savings are going up in detecting a production failure right after it occurs, to minimize rework to correct the failure, rather than detecting the failure after the product is completed.

Further assurance of product design quality can be provided by an independent testing laboratory. It is empahsized that the independent laboratory should oversee the production testing of the manufacturer, and vouch for these test methods as well as for the quality of the product design. Production failures (i.e., products made not according to design) as well as design inadequacies can lead to hazardous products. A National Conference on Laboratory Evaluation and Accreditation is being developed under the coordination of the National Bureau of Standards to establish procedures to assure, possibly both nationally and internationally, the capabilities of independent testing laboratories in performing defined tests.

But there are many aspects of consumer product use for which there are no defined tests. The National Commission on Product Safety found that for many consumer products there are no published standards (which typically include test methods). The Administration has proposed, with bipartisan support, a Consumer Product Test Methods Act, H.R. 6891," a bill to provide incentives for increasing the amount of information available to consumers respecting consumer products." The Secretary of Commerce, in consultation with the Office of Consumer Affairs, would promote the development, approval, and use of methods for testing for consumer product characteristics whose measurement would be in the interest of consumers. Suppliers could then elect to advertise the results of these authorized tests, and their use of accredited testers. Consumers would receive more useful quantitative information to aid their choices in the marketplace. The supplier reporting on a test in advertising or elsewhere would be required to fairly disclose the complete results of such testing. This legislation could provide a measurement language for the consumer interest, and be an important element in providing the buyer's right to the information that would allow intelligent choice in the marketplace.

THE RETAILER

The retailer today takes a limited responsibility for the safety of the products he sells. Only a few of the large retail chains (for example, Sears Roebuck, J. C. Penney's, and Macy's) have their own testing laboratories, and these are used more for buying decisions than for continuous quality control checks. One may note that the second largest United States retailer, the Armed Forces Post Exchange systems, are not prominent for the testing of the products they sell.

At best, the retailer passes on the manufacturer's information to the consumer, perhaps confirming some of it. More typically, the retailer is lost in the information retrieval problem, and gives the consumer only partial answers if not wrong ones.

Some retailers, particularly in their repair operations, are utilizing microfilm or microfiche data systems to rapidly select from large amounts of information the particular model and part of interest. I foresee a further growth of manufacturer information retrieval with the development of computer information and data systems, already beginning to be used for inventory and customer charging purposes. It is a small step for the salesman who can use a computer to see if he has a given model and color in stock for him also to search data supplied by the manufacturer to see the characteristics of that model. At that point, the salesman becomes the tutor of the consumer in the searching for data to allow intelligent choice. Advertising would emphasize information transfer.

THE CONSUMER

Many consumers, of course, will still elect an uninvolved contact with the marketplace, buying on whim, buying on short-term emotional interests which have no place for risk calculations. We cannot make the world "safe", but we can try to make it safer, and education can show the benefits of this effort. With half of today's highschool graduates taking some college work, and with the efforts of Mrs. Virginia Knauer and the Office of Consumer Affairs to increase consumer education, the day of the wise consumer, consumptorem prudentem, may be at hand. We speed the day by asking for information to allow intelligent choice.

What is the waste today of a marketpalce in which the consumer does not have full information to allow intelligent choice? Of the $700 billion spent by consumers for goods and services, how much is spent unwisely, not satisfying the need that would have been satisfied if we had the information for intelligent choice? How many frauds do we suffer, how many wrong repairs are made, how many wrong services are performed, how often do we buy the wrong product? If we include only the difference in cost of the satisfaction of what we bought and what we would have bought if we had had information for intelligent choice, are we 85 percent right in our purchases? Perhaps indeed we are not that successful. Each of us should reexamine his goals and see what information he lacks in making choices in the marketplace to attain them. That 15% that we may be wrong (unnecessarily unsatisfied) is $100 billion, so the buyer's right to information has a golden benefit indeed, and significant costs to insure this right are justified.

THE REPAIRER

Complex products may become unsafe in unsuspected ways with attempts at repair. The necessary trend is that the repairer become increasingly professional, foliowing standards and certifying successful testing of his work. The manufacturer, concerned about his liability, will want to know the repairer's effect on the product and may best protect his name by providing repair services.

THE DISPOSER

Products must increasingly be made with disposal and recycling in mind. This must be planned in the design; the manufacturer may well be the one who should have the responsibility for efficient disposal and reuse. The practice should be encouraged that when a new product is received, the old one is taken away.

TRADE AND PROFESSIONAL ORGANIZATIONS

These bodies have represented the narrowly defined interests of their constituents, but are increasingly recognizing broader social responsibilities as well. Let them speak out on product safety, organizing the special experiences of their members.

NATIONAL AND INTERNATIONAL STANDARDS BODIES

Standards and test methods are the necessary language of informed choice. Even with some 19,000 U.S. voluntary engineering standards, (12) published by some 360 U.S. technical societies, professional organizations, and

trade associations, the consumer standards needs have just begun to be emphasized. Growing world trade is aided by international standards (13) and the "multi-partite" agreements to accept test results across national borders.

GOVERNMENTS

State and local governments, with their building codes, electrical codes, and other regulations have an increasing influence on local commerce. The issue of preemption of local mandatory standards by Federal mandatory standards, even when the Federal standard is weaker, is not finally settled by legislatures or courts. Communication is important to minimize differences; the National Bureau of Standards secretariats of the National Conference of Weights and Measures and the National Conference of States on Building Codes and Standards have been quite successful in helping to draft the Model State Packaging and Labeling Regulation, The Model State Lumber Regulation, and in preliminary efforts to consolidate building codes and redirect them toward performance criteria to allow use of new methods for Project Breakthrough. (14)

Communication cannot erase regional needs for differences of regulation to deal with regional problems of very low temperature, earthquake, hurricanes, etc. The courts, considering preemption, may be expected to respect these needs. The challenge is to write the Federal regulation to include these special circumstances.

But how far a state can get ahead of the nation in general safety requirements remains an issue of our time. Minnesota's efforts to place the emission standards below the Federal standards for nuclear power plants have thus far been denied in the courts.* Consumers may indeed develop local values and wish to defend them by local standards, if these are not recognized by the Federal Regulation.

The Federal Trade Commission is increasing its communication with local consumer protection groups, establishing in many areas Consumer Protection Coordinating Committees (7) of local district attorneys, attorneys general, consumer protection offices, Federal inspectors, weights and measures people, law enforcement people, etc., to insure that local needs are recognized in Washington, and successful methods are shared.

COMMUNICATION

The complexity of the "safety system" that affects the safety of consumer products is such that an interactive computer Product Information Service is essential to let the many participants in the safety system keep up with the many changes and have access to the inclusive representations of problems and data. An interactive computer system lets the user receive an answer to his question, and not have to sort this answer from page after page of printed text selected to answer many questions. A prototype system was the Consumer Product Safety Index (15), although this never reached the interactive stage.

The service should receive from participants (each of whom would sign his name, organization, and date of input) information on

- injury statistics
- case histories (without privacy aspects)
- economic data (products in use)
- demographic data (user characteristics)
- complaints and analyses
- products
- technical information (publications)
- possibilities for product improvements (patents, etc.)
- standards
- benefit-cost analyses of mandatory standards
- legislation
- court actions
- professional people involved (addresses and phone numbers)
- manufacturers
- testing laboratories

and other information needed to make and choose the safer and more useful products that the informed consumer will wish to buy. The system would be intimately cross indexed and subject indexed, so that ideas would lead to related ideas, and each of us would not have to rediscover elsewhere what others of us have found and entered into the system.

*Northern States Power Co. v. Minnesota, U.S. District Court, Minnesota, December 22, 1970. See 39 Law Week 2367, 2368, January 12, 1971.

Now we have, as Thoreau said, the matter of "putting foundations" under our "castles in the air." What does it cost you not to know these things?

CONCLUSION

The world is significantly less safe because most of us are not aware of our hazards. With computer information techniques, the convenience of identifying these hazards will allow us to use this knowledge to reduce our hazards. How thoroughly we act with knowledge may yet determine the survival of mankind. As H. G. Wells put it (Outline of History, 1920), "Human history becomes more and more a race between education and catastrophy."

REFERENCES

(1) Morris Kaplan. Does the Informed Consumer Exist? Will He Ever? Annual Meeting of the National Academy of Engineering, Symposium and Workshops on Product Quality, Performance, and Cost, April 29-30, 1971. National Academy of Engineering, 2101 Constitution Avenue, N.W., Washington, D.C. 20418.

(2) National Commission on Product Safety. Supplemental Studies Volume 2, Industry Self-Regulation. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, June 1970, Price $3.75.

(3) Carl C. Clark. Manufacturer and Government Roles in Consumer Product Design. Boston Section Meeting, American Society of Mechanical Engineers, Massachusetts Institute of Technology, March 18, 1971.

(4) U.S. Bureau of the Census. Vital Statistics of the United States. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, 1969. See Volume 2, Part B, Mortality, 1967.

(5) U.S. Bureau of the Census. Historical Statistics of the United States, Colonial Times to 1957. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C.

(6) Howard Heffron, Richard Medalie, Stephan Kurzman, and Marian Pearlman. Federal Consumer Safety Legislation, A Study of the Scope and Adequacy of the Automobile Safety, Flammable Fabrics, and Hazardous Substances Programs, A special report prepared for the National Commission on Product Safety. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, June, 1970, Price $1.25.

(7) President Richard M. Nixon. Consumer Message to Congress, February 24, 1971. Presidential Report, Volume 9, P. 485-488, February 26, 1971. Available from Mrs. Virginia Knauer, Office of Consumer Affairs, Executive Office of the President, Washington, D.C. 20506, 202-456-2645.

(8) Lewis M. Branscomb. Product Performance in An Affluent Society, Annual Meeting of the National Academy of Engineering, on Product Quality, Performance, and Cost, April 29, 1971. Available from the National Bureau of Standards, Washington, D.C. 20234.

(9) Carl C. Clark. Safety System Dynamics for Consumer Products - Some Factors Affecting Decisions About Safety. 21st. Annual Appliance Technical Conference, Institute of Electrical and Electronics Engineers, May 1970. IEEE Transactions on Industry and General Applications, Vol. IGA - 6, No. 6. P. 534 - 539, November/December 1970. See also the American Society of Safety Engineers Journal, Vol. 15, No. 10, P. 17 - 23, October 1970.

(10) Department of Defense. Military Standard MIL-STD-105D, Sampling Procedures and Tables for Inspection by Attributes. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, 20 April 1963, Price 40 cents.

(11) National Commission on Product Safety. Final Report. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, June 1970, Price $1.75.

(12) William J. Slattery, Editor. An Index of U.S. Voluntary Engineering Standards, National Bureau of Standards Special

Publication 329. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, March 1971, Price $9.00.

(13) Daniel V. De Simone, Director, U.S. Metric Study. International Standards. National Bureau of Standards Special Publication 345-1. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, Price $1.25.

(14) National Bureau of Standards. NBS Technical Highlights, 1970. NBS Special Publication 340. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, February 1971, Price $1.50.

(15) Carl C. Clark and G. Michael Smith, Editors. Consumer Product Safety Index, of the National Commission on Product Safety. Computer system printout, 3000 pages in 3 volumes, July 1970. Order documents PB-193 425, PB-193 426, and PB-193 427, Price $30., for the full size page copy, or document PB-193 428, Price $10., for the microfilm copy, from the National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22151, 703-321-8543.

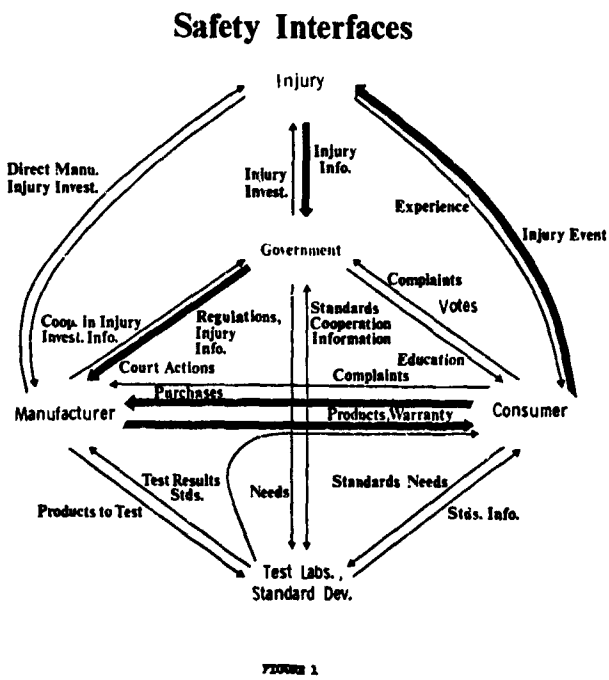


FIGURE 1

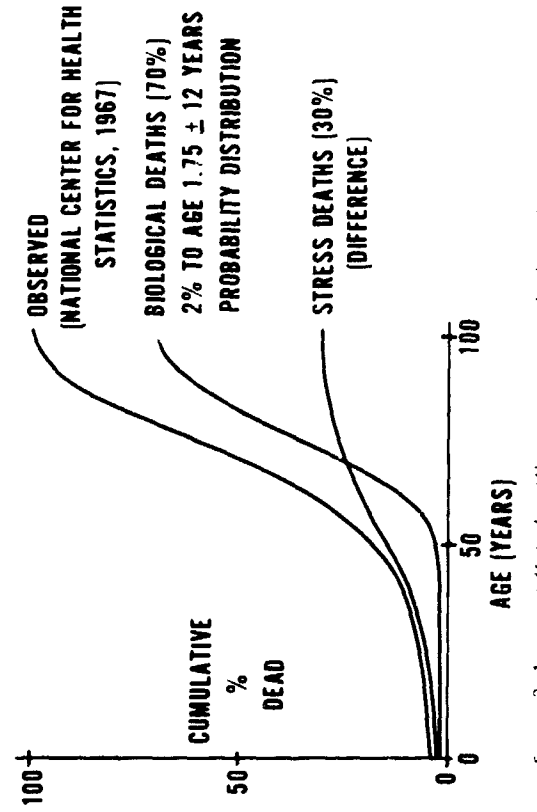


Figure 2 A curve fitting hypothesis concerning biological and stress deaths

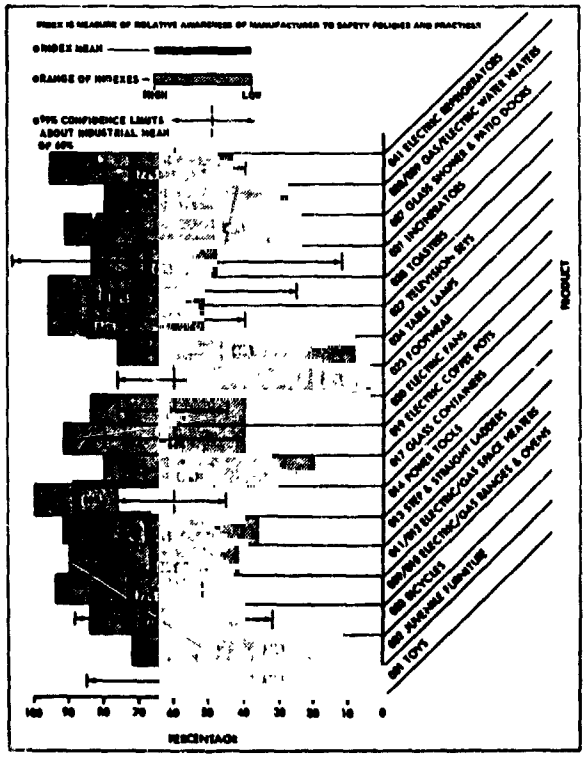


Figure 3 Average Index For Manufacturers Product Code

N72-25983

APPLICATION OF SYSTEM SAFETY

TO

RAIL TRANSIT SYSTEMS

By

Mr. Thomas DeW. Styles
Chief
Railroad Safety Division
National Transportation Safety Board
Department of Transportation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

Rail rapid transit, as we know it today, came into being shortly after the turn of the century. Although inter-city railroad passenger service was well established and thriving, the opening of New York City's first subway in 1904 was the beginning of rail rapid transit in this country. Since that time, development of the rail rapid transit industry has been sporadic. Until very recently most activity took place prior to World War II.

The term rail rapid transit as used in this paper refers to systems, excluding streetcars, that utilize single or multiple-unit trains on a two-rail track. As used here rail rapid transit includes subway, surface, and eleveated trains operated by public or private transit authorities as well as commuter-trains operated by railway companies.

The current urban renewal activity and emphasis on community planning and improvement has brought about a change in urban transportation philosophy. Once again, the modernization and expansion of rail rapid transit systems and the construction of entire new systems is underway. Large scale improvements and expansions are being planned or made to the systems in Boston, New York, Philadelphia, Chicago, and Cleveland. New commuter cars are being purchase for use in the New York area on railroads and in the subway system, and on the railroads in the Philadelphia area, and in Chicago. Complete new automated rail rapid transit systems are being built in San Francisco and here in the Washington metropolitan area. A successful automated system has been running for more than a year between Lindenwold, New Jersey and center city Philadelphia. Plans for rapid transit are in various stages of development in Atlanta, Baltimore, Los Angeles, and Seattle, while Pittsburgh's plans embrace an intermodal concept which includes the so called "Skybus."

The availability of Federal funds has been a moving factor in this rebirth. The Urban Mass Transportation Act of 1964 offered the first continuing program for urban mass transportation. The Urban Mass Transportation Act of 1970 continues and expands the role of the Federal Government by authorizing 3.1 billion dollars for mass transportation during the next five years. The 1970 Act also expresses the intention of the Congress to provide 10 billion dollars in assistance over the next 12 years. In addition to Federal grants, a marked increase in the financial participation of State and local governments has occurred, with the prospects of additional funds in the future.

The Urban Mass Transportation Act of 1970 includes as part of its purpose the word "safe." The meaning of the word safe is not spelled out in the Act; however, we at the National Transportation Safety Board have definite feelings about the future meaning of the word and will make some recommendations to UMTA regarding its implementation. These recommendations are the result of several months' observations made by Safety Board personnel of transit operations in New York, Philadelphia, and Chicago. These observations were supplemented by consultation ith the personnel of the Metropolitan Transportation Authority, the Port Authority, and Penn Central Transportation Company in New York; the Southeastern Pennsylvania Transportation Authority, the Port Authority Transit Company, the Reading Company, and the Penn Central Transportation Company in Philadelphia.

Let me clarify one thing at this point. The rail rapid transit industry historically has been considered a safe method of urban transportation. Recently among the older systems this image has been tarnished by highly publicized incidents of system failures. In spite of these system failures, and in spite of the absence of statistical data to confirm it, passengers on board a rapid transit train are exposed to a much lower risk than on any form of highway travel.

There is no single private or governmental agency to which all of the rail rapid transit industry reports comprehensive accident data on a regular basis. Railroads and certain of the interstate transit authorities are required to report accidents to the Federal Railroad Administration; however, the methods are oriented to conventional railroad operations with no separation for commuter operations.

Within the transit industry, the American Transit Association compiles operating accident statistics for transit systems but includes only motor coach, trolley coach, and street car operations. Recently, there has been an effort by the transit members of the National Safety Council to establish a uniform system of compiling and exchanging accident

information, but there has not been uniform acceptance of these procedures. The net result is a complete lack of data that can be used as a comparison of safety within the industry or between transportation modes. When one does not know the characteristics of the accidents and where they are happening, and both accident and use history data are not available, operations analysis to identify problems areas becomes difficult.

Rail rapid transit systems and railroads are good examples of the highly wasteful, but normally used approach which attacks problems as they are revealed by accidents. Within the present state-of-the-art it is most inefficient to wait for the accidents to occur and then to correct the problems by making changes. Obviously what should be done, of course, is to find the hazards in advance. Through systematic analysis of the system one may predict the likelihood that those hazards will be activated by exposure of the system to a system failure, a human error, conditions external to the system, or combinations of these; determine the alternatives to the assumption of this risk; and recommend the corrections before the system is put into operation.

The problem becomes one of indoctrinating this concept into the rail rapid transit industry. Historically, the rail rapid transit industry has depended on a good past accident record rather than focusing on means for identifying hazards and evaluating risks. There appears to be an attitude in the railroad and transit community that no professional engineer would design or produce an unsafe product, and I agree that no professional would knowingly do this. However, there are concrete examples in the transit field today where these safety-conscious professionals have produced components that resulted in a system that contained hazards which could lead to disaster if they had not been found.

These examples of hazards are physical evidence that the application of a disciplined, systematic review of a system is necessary if optimum safety is to be accomplished. A review of some of these conditions will illustrate the applicability of system safety to the rail rapid transit industry.

Station accidents represent the highest accident ratio in the industry and include falls on stairs, escalators, platforms and passageways, injuries from assault or being pushed by other persons, and injuries resulting from smoke and other miscellaneous causes.

The facilities involved in most station accidents are also those that receive substantial architectural consideration during construction or modernization programs. Too often the aesthetic viewpoint dominates the practical considerations. Open stairwells and barrier-free escalator handholds challenge the acrobatic capabilities of children. Street entrances are often sloping ramps that resemble ski slopes during snowy winter weather. Subdued lighting in entrances greets patrons wearing sun glasses. Wall and ceiling surfaces are covered with material which quickly lose their reflectivity upon exposure to rail and wheel dust and the graffiti experts.

It is significant to note that the highest incidence of fatality in rail rapid transit does not occur to the passenger on board the train but to persons on the track, including trespassers and those who have jumped from station platforms or were inadvertently pushed.

The train-person collision, where it involves patrons, occurs in the proximity of station platforms and is most frequent at car-floor height platforms. Station accidents involving a fall to the track are also experienced at these locations. In spite of this experience, the trend in the industry is towards open, car-floor height platforms to enhance faster discharge and receipt of passengers. In our society there are very few places where the public is allowed to congregate immediately adjacent to an unprotected opening four feet deep. This is the case where commuters jostle each other on high-level platforms while waiting for rapid transit trains. To increase the hazard, trains pass through the opening at speeds up to 75 miles per hour.

In most older systems, if a patron were pushed, fell, or jumped to the track the possibility of being hit by a train was minimized, to some extent, by the use of express tracks which were separated horizontally from car-floor height platforms. The newer systems are not utilizing this concept and nonstop trains whiz by crowded platforms. Platforms now are located also in the median strips of crowded expressways where noise and other distractions are prevalent. Warning systems are not

provided and therefore the likelihood of a train approaching without detection has increased markedly. Architectural considerations in new underground stations have dictated that the track zone be sparsely lighted so that unaesthetic views of the track are not highlighted. Therefore, a person who has fallen on the track is obscured by shadows and is less likely to be seen.

Further, train-person collisions are experienced at surface stations constructed with low, rail-height platforms. The majority of these accidents involve patrons taking short cuts across tracks which either have no intertrack barriers or barriers inadequate to discourage this practice. Unfortunately, many at-grade stations have highway grade crossings at one end or the other of the station platform that make the erection of permanent effective intertrack barriers extremely difficult.

Grade crossings are not compatible with rail rapid transit operations. The consequences of a collision of a rail rapid transit train with a truck load of hazardous materials could be a major disaster. In December, 1966 at Everett, Massachusetts a rail commuter car struck a stalled tank truck of fuel oil and the resulting fire killed 13 persons because they could not escape from the car. There were no emergency exits and the inward-swinging door was jammed closed by the press of the people trying to escape the fire. It takes very little imagination to see what could happen to a commuter train with several hundred persons on it if it struck and ruptured a tank truck of gasoline or liquefied petroleum gas.

Grade crossing protection or elimination programs have been unorganized, dependent in many instances, not on the hazards involved, but on whether the road involved is classified as a "Federal Aid" route. Motor vehicle laws involving grade crossings are ignored by the general public and not enforced by local authorities. Zoning laws and other local ordinances are explicit in their requirement to insure compliance with environmental and other social values. These regulations also generally prohibit sight obstructions at street intersections. It is rare, however, to find any regulations affecting the type of construction or landscaping in the vicinity of a highway-rail grade crossing.

Although grade crossing accidents are recognized as a hazard within the rail rapid transit industry, in some instances the design of the car equipment is not consistent with this recognition. Transit cars originally designed for operation in a closed system are operated over highway grade crossings. The pilot protection, deemed necessary in the railroad industry to minimize the chance of derailment upon hitting an obstruction, is not provided consistently on rail rapid transit cars. In some instances, passengers are seated at the front of the car immediately adjacent to a large windshield. In the event of a grade crossing accident, the passengers will have an excellent view of the event if they survive to relate it.

Injuries that have occurred in the on-board category have involved or resulted from boarding and alighting; falls on board, including falls between cars; vandalism; fire or smoke; and to a lesser extent, derailments or collisions. Original design has been a factor in all of these incidents.

Boarding and alighting accidents have involved the car doors, the space between the platform and the car, open spaces between cars, the car steps and the platform surface. As a general rule, car-floor height platforms were observed more in inner-city type operations, with low rail-height platforms being provided at locations handling suburban service. The experience again indicates a lower accident frequency at low platforms than at the car-floor height platforms.

New car equipment has been observed with no protection provided for the space between cars. This has resulted in falls to the track while boarding or alighting as well as on-board falls. Understandably, the results have generally been severe. Protection has been provided with intercar chains as well as retractable gates, both of which appear to be only a partial solution added as an afterthought.

On several systems car-floor height platforms are inter-mixed with those of low rail-height design. To accomodate boarding-and discharge this has necessitated car vestibules with trap doors in the down-position for car-floor height platforms and in the up position for the low platforms. The trap door has been the source of numerous injuries and its use should be discouraged.

I think we can assume that in rush hours there will be a large number of standees;

however, minimizing the number of standees will reduce the number of on-board falls. The provision of hand holds designed for passenger comfort and convenience should be reconsidered. Improved car suspension systems and smoother accelerating and braking characteristics would be helpful also.

Some of the newer commuter cars have the "flop-over" seats so that when the train reverses direction, the seat backs are "flopped over" to allow the passenger to ride facing forward. There have been instances where emergency stops have been made resulting in the standees grabbing the seat backs to prevent themselves from falling. This "flops over" the seat backs with passengers sitting in them. An analysis of this feature would have revealed the obvious hazard in this type seat arrangement.

Obviously, there are many operating factors which affected the design of rail rapid transit cars. Safety should be given high priority as a factor.

Window designs vary from the large picture window to the porthole type. Almost all transit passengers face the hazard of being injured by thrown objects, and design of windows can lessen the severity of injuries from thrown objects. Various types of glass panes are used and now tough plastic material which will withstand the impact of a thrown rock is being used.

The design of the front end of transit cars can influence the severity of a grade crossing collision. Large expanses of glass on the front ends of cars subject the operator and passengers to additional dangers from impacts of objects thrown from above as well as collisions at grade crossings.

There appears to have been no systematic approach to the design and use of windows. The obvious approach would be to determine the environmental exposure of the windows and surrounding structures during their operational life-time. Once these environments are understood, the optimum combination of window pane and surrounding structure can be determined as those which offer the least risk to the passengers and crew.

Although window design is the most conspicuous, there are many other car design areas that warrant re-examination for determination of the optimum design. These design characteristics vary in importance and include in part: exit location and design, passenger seating arrangements, accommodation of hand-luggage, motorman separation, intra-car passageways and barriers, rear-end illumination, front-end derailment and collision protection, braking systems, car-wheel metallurgy, and automatic control systems.

While new rail rapid transit cars are subject to differences in design criteria between systems, they also contain common innovations which are valuable in furthering passenger safety. These include such items as two-way radios or train-phones, complete train public-address systems, speedometers, improved ventilating systems, and emergency car lighting. The installation of these devices has been accomplished with safety in mind; however, experience has provided the hazard analysis.

As in other transportation networks, the traffic-control system of rail rapid transit is a necessity in the safety and effiency of operations. Unlike other transportation networks, however, a train must stay with the route established for it by the track and the traffic control system. The engineer does not have the option of selecting an alternative route at the last moment when an accident appears imminent. Therefore, both safety and reliability must be designed and built into the traffic control system as a prerequisite to efficient operation without a high accident frequency rate.

Although railroad and transit accident statistics indicate that the failure of signal systems does not cause a significant number of accidents, much can be done in the field of signals to enhance railroad and transit safety. Many accidents attributed to man failure and acts of God can be prevented by a good signal and train control system. The modernization, and extension of existing lines appears to perpetuate existing signal systems without due regard to the accident experience of the system involved.

New rail rapid transit lines are being designed with the capability of a fully automated signal and train control system. These new systems should be subjected to rigorous safety analyses to assure that the system will operate safely for a prolonged period of time under varied maintenance conditions. The analysis of a computerized system using digital data inputs requires the application of sophisticated safety analysis techniques.

Almost invariably rail rapid transit tunnel design shown lack of foresight in providing for emergency situations. Minor smoke or fire incidents in tunnels have turned into panic situations, resulting in injuries and loss of life.

Safety walks originally intended for use in the evacuation of passengers have been utilized to accommodate signal and electrical facilities. Walks are also used for the storage of maintenance of way material. Emergency exits have been located immediately adjacent to turnouts presenting an obstacle course of running rails, guard rails and energized third rails. Exits are sparsely located and difficult to identify under normal circumstances, both inside and outside of the tunnels. Exits are narrow and steep, easily negotiable by a spry young man, but another matter for a not-so-spry elderly lady. In some instances, in-tunnel lighting is practically non-existent and ventilation is dependent upon natural drafts. The hazards of tunnel evacuation are recognized in existing rule books that indicate that detraining of passengers within tunnels must only be accomplished as a last resort.

The minimization of the hazards in existing emergency tunnel evacuation is an area that demands immediate attention. Upgrading programs have been undertaken on some systems and the results are markedly apparent, although no one system has accomplished all of the following steps. The steps that have been taken to improve conditions include the installation of additional lighting, signs, emergency telephones, fire alarms, power disconnects, handrails and fire extinguishers. Portable emergency equipment such as de-training ladders, bull-horn speakers, stretchers, lanterns, air-paks, first-aid kits, and between-rail walkways have been strategically located either in tunnels, at stations, or on equipment. The installation of this type of equipment is mandatory if operational delays, adverse publicity, lawsuits and most important, loss of life are to be minimized.

Closely related to the tunnel design problem is that of the third rail. The third rail conducts the electric power for the operation of most rail rapid transit cars. In most instances, the third rail carries 600 volts of direct-current power and is located immediately adjacent to the tracks. The third rail has been a source of electrical burns and fatalities for passengers, trespassers and employees even though in both of the two basic designs, under-running and over-running, some protection against electrical shock has generally been provided. The third rail and the associated connecting appurtenances on the transit car have initiated fire and smoke incidents. Generally, the fire and smoke injuries have been relatively minor, but serious accidents have been caused by subsequent detraining and evacuation. For new systems this design warrants a complete reappraisal.

Rail rapid transit construction recently has shown increased usage of the joint-corridor concept, sharing right-of-way with existing or new highways or railroads because of economic and social considerations. This concept has many proponents and the arguments for joint utilization are indeed convincing.

The safety of each mode must be assured at an interface such at this and to accomplish this requires a systematic evaluation of the hazards of each mode and the interface between the modes. These evaluations must be made in the planning stage rather than after the system has been constructed and alternative plans are too expensive to implement.

When one looks at the possibility of a gasoline or liquefied petroleum gas tank truck violating the transit track space the potential consequences are frightening. A comparable prospect exists where rapid transit tracks operate jointly or adjacent to a freight-carrying railroad. Shifted loads and derailments can foul the transit tracks resulting in catastrophic collisions.

I would be shocked genuinely to find a transit operation without a safety department. I would expect to find that safety is deemed the first responsibility of all employees, and each supervisor is charged with the responsibility for safe operations within its jurisdiction. For the most part, however, management emphasis on safety involves employee activities. It would be completely unfair to imply that there is a lack of concern for passenger safety within the rail rapid transit industry. There are concentrated efforts to investigate accidents and improve the lot of the passenger; however, these efforts did not appear to receive the emphasis that was regularly placed on employee safety by the safety departments.

Safety department personnel generally are charged with the responsibility of "closing the barn door after the horse was stolen" without having an opportunity to review a new facility during design and construction. The safety input for new or modernized facilities has been accomplished historically by the design engineers and/or operating and maintenance personnel. While these groups surely have safety in mind, they are influenced also by architectural, operating, maintenance, and economic considerations. A system safety review of new or modernized facilities normally does not take place during the conceptual stage. As a result, it has not been unusual for new facilities to be modified after they are operational and the first accident occurs, at a cost that is greatly in excess of that required to remove the hazard from the initial design. Safety personnel are not used to the extent of their potential, which I understand is not a new situation.

There is a ready application for system in the rail rapid transit field and the time to start is now. The degree of safety achieved in any system is directly dependent upon the emphasis of management. In the rapid transit industry this management emphasis on safety includes the management of the granting and use of funds by the Federal Government. This management emphasis must be applied during the conception, development, production, and operation of each system throughout its life cycle.

Much needs to be done with the existing operating systems. System safety programs for new systems are not the only needs in the industry. Keen analyses of the present systems would identify the hazards and evaluate the corrective actions so that management could determine what degree of safety is needed. The public which is paying the bills can no longer afford the inefficient method of waiting for an accident to occur and then correcting the problem.

N72-25984

DESIGNING FOR AUTO SAFETY

By

Mr. Elwood T. Driver
Director
Office of Operating Systems
Motor Vehicle Programs
National Highway Traffic Safety Administration
Department of Transportation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

Thank you, it's nice to be back and to have the opportunity to bring you up-to-date on what's new in the field of auto safety; especially in the area of design, since all vehicle manufacturers must translate our Federal Motor Vehicle Safety Standards into designs that meet the safety performance requirements.

First, I'd like to show you some figures and discuss how our activity has been reflected to these safety statistics. Much has happened in the field of motor vehicle safety since I spoke to you on May 1, 1968. Later we'll explore what's in store for the next two or three years in the motor vehicle and highway safety field.

Figure 1 shows the traffic situation today. From 1961 through 1966 the average increase in fatalities was 6.8% per year. However, since the expanded Federal Safety Program got under way, this trend has dropped to 0.95%--in spite of a 6% increase in vehicle registrations and drivers and a 4% per year jump in total miles driven. These fatality figures represent a startling drop when you consider that only about 1/3 of all the cars on the road today have the new safety features.

Our early projections indicated that the number of crash victims should start to decline around 1972 or 1973. However, last year, 1970, we had 2% fewer deaths than in 1969 (56,400 vs 55,300). We believe the tide has begun to turn. Additionally, recently tabulated data shows a decline in severity of injury, as reflected in the number of days lost through reduced activity and hospitalization because of motor vehicle crashes. The rate rose sharply until 1966. For example, in 1967, an average of 34 days was lost due to restricted activity while in 1969, this average was down to about 25 days.

Evidence that later model cars are safer is shown in a study, made by the Highway Safety Research Center, University of North Carolina, of injuries to drivers in 270,000 vehicles involved in accidents in North Carolina from 1966 to 1968. Results suggest that for every 100 serious and fatal driver injuries in 1968 models, 130 would have occurred in a similar array of crashes had 1966 models been involved. The Director of the HSRC states that, "as more and more of the newer cars, with more safety devices, come onto the highways, there will be a more pronounced safety factor to work against the upward pressures from more cars, more miles and higher speeds."

Figure 2, our systems approach, which I described to you 3 years ago, has begun to pay off. Let's take a look at one of the old system description slides. By using a systems approach to prevent or lessen the end results of deaths, injury and property damage, we must either.

1. Prevent the occurrence of crashes: - Precrash
2. Increase survivability in crashes that do occur: - Crash
3. Provide prompt medical attention to injured people and other postcrash salvage measures: - Postcrash.

The systems approach (Figure 3) on the time base precrash, crash and postcrash, is interfaced with the system elements of the driver, the vehicle and the environment. Of these three systems, action on the vehicle system will effect the greatest and quickest pay off. Design modification will reduce the national emergency proportions of highway deaths, injuries and crashes. In working to make these design changes, we deal with a small number of American and foreign vehicle manufacturers to effect the safety changes.

Vehicle design is the most direct and most positive means for man to affect system safety in the shortest time. We (MVP) can do many things with vehicle design to keep the driver out of trouble and make sure that he does not pay with his life for his first mistake.

Our enviable highway network contains millions of miles of roadway under local, State and Federal jurisdiction. The Federal Highway Administration and Traffic Safety Programs, a part of D.O.T., are concerned with the vehicle environment or roadway. They direct their system effort to safer roadways by improving traffic capacity, sight distances, speed, lighting; removing roadside hazards and accident-producing obstacles, controlling safer traffic flow through better signs, signals and computer control systems. The time frame for this systems approach, as you know, is longer than the vehicle approach.

Altering or changing the third system, the driver, is also a long term approach. With some 111 million licensed drivers, most

good, some bad, operating 111 million vehicles over 3.7 million miles of roads in 51 separate jurisdictions, you can readily see that the education, training, licensing, and record keeping of vehicle drivers could not have a fast payoff. The basic responsibilities for safe operation of highway traffic and for control of drivers remains with the States.

Last month in Detroit, a high speed crash on the Edsel Ford Expressway (Figure 4) illustrates the simultaneous contribution of all three systems to a deadly crash:

1. The Driver
2. The Vehicle
3. The Environment.

While our systems approach is basically unchanged, the organization which implements the system has changed in structure and size.

Since I was last here in 1968, (Figures 5, 6, 7, 8, 9, & 10) the National Highway Safety Bureau has come of age and is now a full fledged Administration - the National Highway Traffic Safety Administration. This Administration is organized as shown with Motor Vehicle Programs being responsible for the development and issuance of safety standards. Here we see the organization of Motor Vehicle Programs and the three Offices assigned to preparing standards. Operating Systems, Crashworthiness and Vehicles in Use. In the two other Offices shown - Defects Review is concerned with investigating and following up on problems affecting the operation of vehicles in use by the motoring public - such as the Ford lower control arm problem and the G.M. three-piece truck wheel which affected a great number of truck campers. The Other Office - Compliance - is responsible for insuring the compliance of new vehicles and vehicle equipment with the requirements of all safety standards in effect today.

As more and more standards and amendments are issued (Figure 11 & 12) they begin to affect many of the same components and subsystems of a vehicle. It soon became all too apparent that we had to supplement the systems approach in our thinking and subsequent issuance of rulemaking actions. To this end (Figure 13) we now have an Engineering Systems group - a staff function to the Associate Administrator - to insure that all of our standards are properly interfaced with others that affect a common component.

Also (Figure 14) equally important, we now provide for the timely introduction of our standards with effective dates that complement the product cycle operation of the vehicle manufacturers. Also, we now carefully analyze the safety benefits of each new rule as to cost and pay off in terms of reductions in deaths, injuries and accidents. These new approaches insure that new standards will be reasonable, appropriate and practicable.

When I spoke to you in 1968, we had issued 23 standards. These original standards were based, to a large extent, on existing SAE and other existing voluntary standards and various government requirements for vehicle safety. They did not specify, in many cases, the requirement for safety in quantifying terms. We have since addressed ourselves to these deficiencies. For example, Safety Standard No. 104 required a windshield washer and wiper. This has now been upgraded through amendments to specify exact requirements for how much of the windshield must be washed and wiped. The same is true for Safety Standard No. 103 - Windshield Defrosting and Defogging. Since 1968, the original 23 standards have grown to 34 standards, 5 regulations, and 79 amendments. I want to point out that in many cases amending an existing standard is as complicated, if not more so, as issuing a new standard. For example, we recently amended Safety Standard No. 208. This was initially entitled, "Seat Belts." The amended version has been renamed, "Occupant Crash Protection Systems" and now specifies among other things the requirements for passive systems to protect the driver and occupants from injury in the event of a crash. A tremendous effort was required to promulgate this amendment.

The systems approach here points up the validity of our emphasis on the vehicle rather than the driver to achieve a reduction in highway fatalities. We have required seat belts in passenger cars since 1968, but we can't make people use them.

The National Safety Council claims that if all available belts were always worn, between 8,000 and 10,000 lives could be saved every year. We also know that seat belts saved 2,000 to 3,000 lives last year; even though only 35 percent of the cars in this country have them.

People say they get "all bunched up" and get in the way. Well, the best way to keep them from being bunched up is to fasten them around your waist! And then they say, "But that's uncomfortable--it restricts me" and to that, I can only say that seat belts are not as uncomfortable as a cast on the leg, and they don't restrict you half as much as a hospital bed does.

However, the trouble is, figures indicate that no more than 30 percent of the public uses its lap belts and only a paltry 4 percent uses the shoulder harness. So it is quite evident that we need a method which does not depend upon any action that must be taken by the driver or his passengers. So we are going all out for a passive restraint system. The leading type of these is called the "Air Bag." I've seen them work and I'm convinced that they can do the job.

I would be the first one to concede that improving the car alone will not end all road fatalities. We are dealing with a complex system of man, machine, and highway. We have to hit all three hard in a coordinated attack if we are going to start saving those 55,000 lives being thrown away every year (as revealed by the latest compilation of figures we have at D.O.T.). In addition to a better machine, we need to complete our Interstate system because for every 5 miles built, we save one life per year--on a continuing basis.

In fact, since the Interstate highway program began, we have saved over 35,000 lives because the Interstate system is that much safer for motorists. Another thing we are going to do is continue to improve the older primary and secondary roads.

But perhaps the major improvements during the 70's are going to be in the area of driver qualifications. Let me give you a profile of a typical accident.

The Profile: The wee hours of a Saturday morning in December are apt to be the most dangerous time of the year for driving...

Death is most apt to occur at that time on an undivided two-lane highway in a suburban area...

The weather will be clear and the victim will probably be a 21-year old male driver alone in a sports car...

The likelihood is that he will run off the road and crash into a tree or utility pole...

He will die, usually instantly, of head and chest injuries...

Tests will show that he had an alcoholic level of .15 of one-percent in his blood--more than half again the Federal government's standard for intoxication.

These are not guesses--these facts come from the results of a $1.2 million Department of Transportation grant to the Commonwealth of Massachusetts to computerize accident data.

The Massachusetts study shows that more than two-thirds of all auto deaths were triggered by alcohol. (We have been using, nationally, the figure of "more than half." The startling Massachusetts figures show that we may have underestimated.)

We estimate that the use of alcohol by drivers and pedestrians causes at least 25,000 deaths and 800,000 injuries each year. The sickening aspect of this tragedy is that so much of the loss of life, limb and property is suffered by people who are completely innocent.

However, public myth has always held that you can't really do very much about the drunken driver. Well, the time has come--in fact, it's overdue--for us to demolish this defeatist attitude. But it will take more than a simple Breathalyzer test.

We have just set up an Office of Alcohol Countermeasures to direct our top-priority campaign in this area. The job of this Office will be to identify the chronic drinker before he becomes a statistic in the morgue--or kills an innocent victim. The alcoholic, contrary to legend, does have an identity. He is on somebody's book, either as a patient, a bad employment risk, or troublemaker or a poor insurance risk. Most heavy drinkers are already known to family counselors, welfare agencies, local traffic courts and their long-suffering neighbors.

So, whenever a man is convicted for drunk driving, his entire background should be investigaged before he is sentenced. The judge should determine whether the offender has ever been arrested before for drunkenness--on or off the highway. Then he can confront him with two options--either get treatment and dry out, or stop driving. Period. No leniency, no excuses, no extenuating circumstances. The tough approach has paid off in

countries as diverse as Sweden and Great Britain.

Much of this talk has concerned new vehicles and new equipment and, if this were our only approach, it would take 11 years of introducing standards on new vehicles to get complete coverage of the vehicle population. To determine the scope and limitations of vehicle-in-use candidate standards, detailed fault logic was used to identify vehicle safety critical systems. This effort is reflected in the Booz-Allen Hamilton Report No. FH-11-7316.

The hazard analysis technique used in aerospace was used during the development of the dual fuel project by General Services Administration with Department of Transportation assistance. This technique was also applied to passive restraint system to a limited degree.

Before closing, I'd like to say a few words about our experimental car project (Figure 15)

The National Traffic and Motor Vehicle Safety Act of 1966 provides that the Secretary of Transportation shall conduct research, development, testing and training on experimental motor cars and equipment.

We have awarded three contracts totaling nearly 8 million dollars for construction of an experimental vehicle. (Figures 16, 17 & 18) A.M.F., Fairchield Hiller and G.M. (their bid was $1.00) have contracts for the production of a 5 passenger, 4-door sedan weighing about 4,000 pounds with a wheelbase of about 120 inches. These low emission vehicles will have three different designs with accident avoidance and crash injury reduction objectives in mind.

We are requiring that the integrity of the passenger compartment should be insured in barrier crashes up to 50 mph, that the compartment should also remain intact in rollovers at 70 mph. These all-new vehicles will enable us to set improved future safety standards for all automobiles offered for sale in this country. One contractor will build and test a total of 14 of these cars by the end of 1972, after a run-off between prototypes.

These mobile laboratories will help provide effective and realistic answers to the problem of cutting the highway death toll.

Three years ago, we were on a rising curve of highway deaths and crashes (Figure 1). By systematically applying our research and knowledge, we have turned the curve downward. With our safety standards, improved restraint systems, alcohol programs, proposed used car programs and our experimental safety cars, we think we can bring all the elements of the safety equation into balance.

We believe we can drive highway fatalities down by 40% by the year 1980. When I say we, I mean all of us - you, the individual driver, the manufacturers, the equipment suppliers, the State regulatory agencies, and the insurance companies.

We will all be driving for the greatest possession of all. We'll be driving for our life.

CRASH SEQUENCE CLASSIFICATION 2

PHASE	SEQUENCE	OBJECTIVE	ILLUSTRATIVE PROBLEMS
PRE-CRASH	1. SELECTION & DEVELOPMENT 2. OPERATING	PREVENTION	● DRUNKEN DRIVING ● ROAD MAINTENANCE ● MECHANICAL & MEDICAL FACTORS
CRASH	1. FIRST COLLISION 2. SECOND COLLISION	AMELIORATION	● CRASH DESIGN: VEHICLE AND HIGHWAY ● SAFETY HELMETS
POST CRASH	1. SIGNAL GENERATION 2. SIGNAL RECIPT 3. RESPONSE-DISPATCH-ARRIVAL 4. LEAVE ACCIDENT SCENE 5. ARRIVAL AT MEDICAL FACILITY	SALVAGE, HUMAN AND PROPERTY	● RAPIDITY & QUALITY OF RESPONSE ● EXTRACTION FROM VEHICLE ● REMOVAL OF DEBRIS ● " ACCIDENT " AND SURVIAL ANALYSIS

FIGURE 2

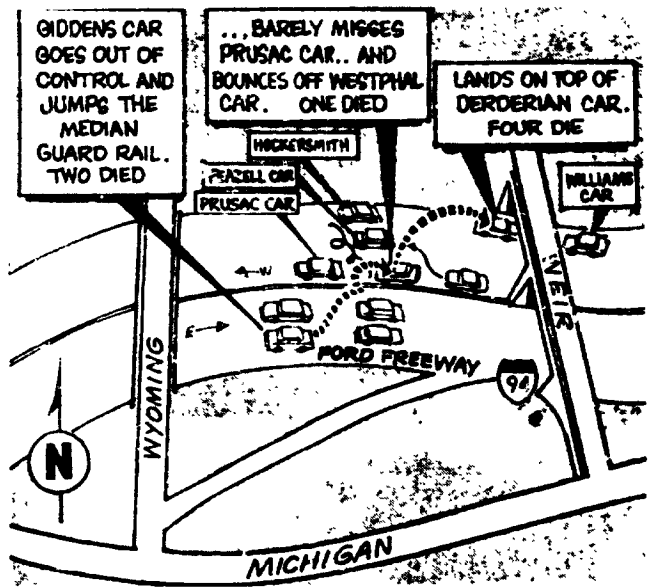


FIGURE 3

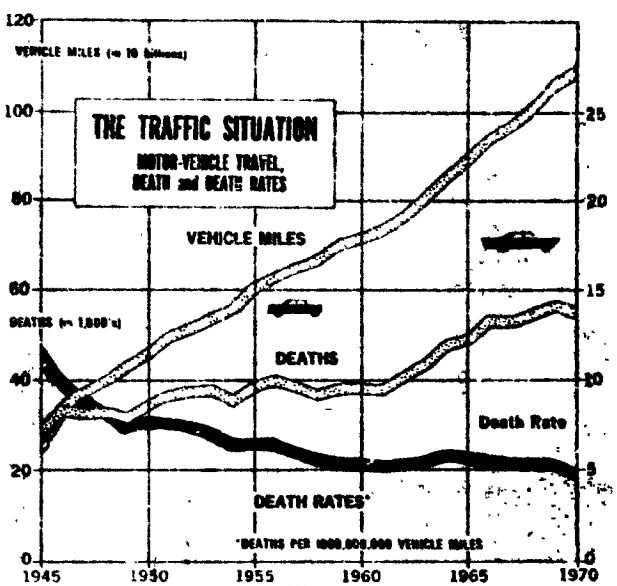


FIGURE 1

FIGURE 4

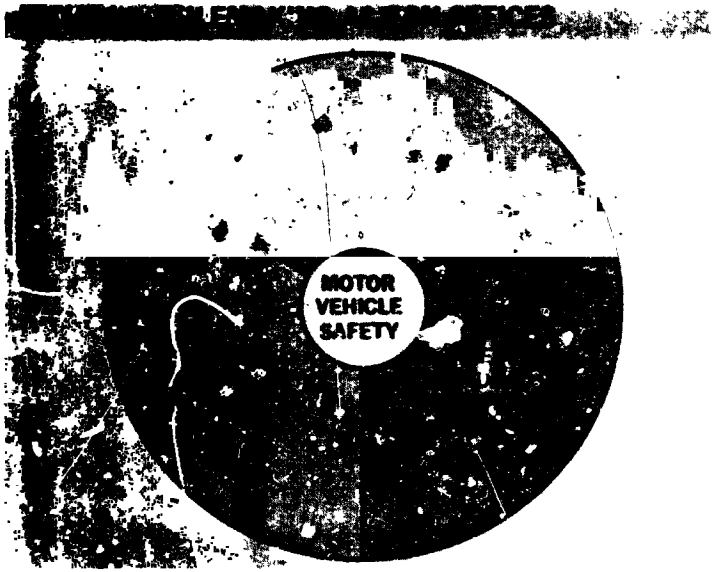


FIGURE 7

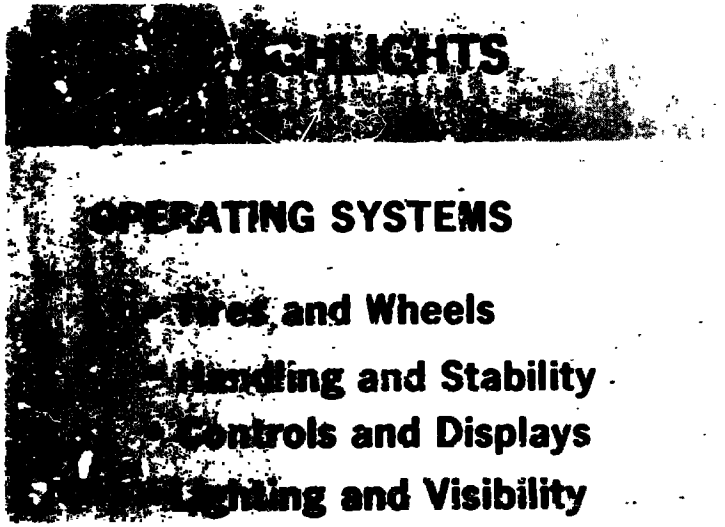


FIGURE 8

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION (NHTSA)

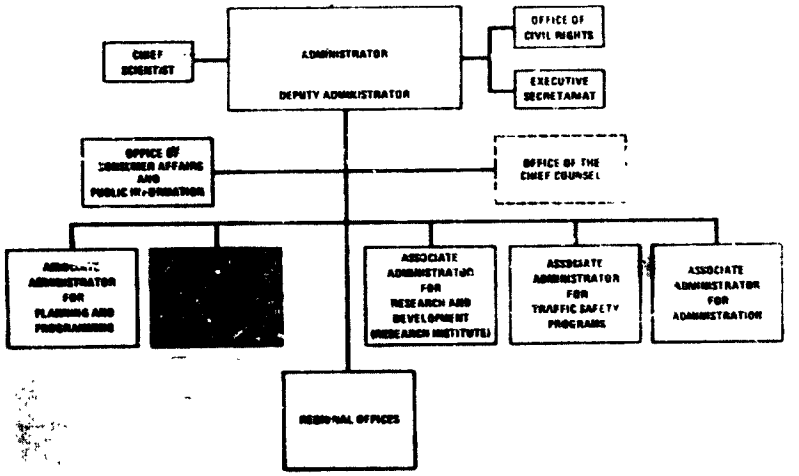


FIGURE 5

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION
MOTOR VEHICLE PROGRAMS (MVP)

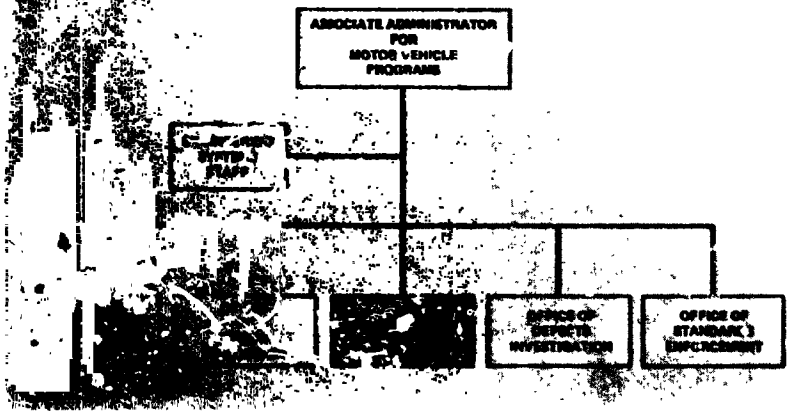


FIGURE 6

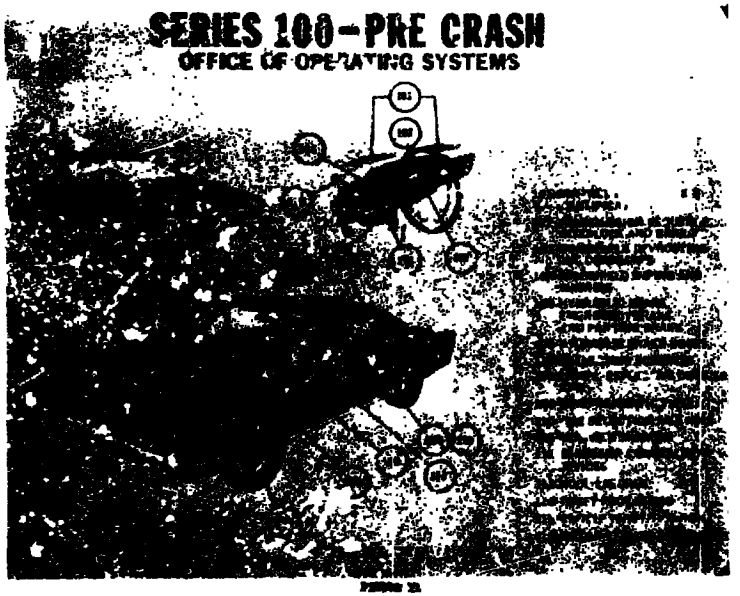


FIGURE 11

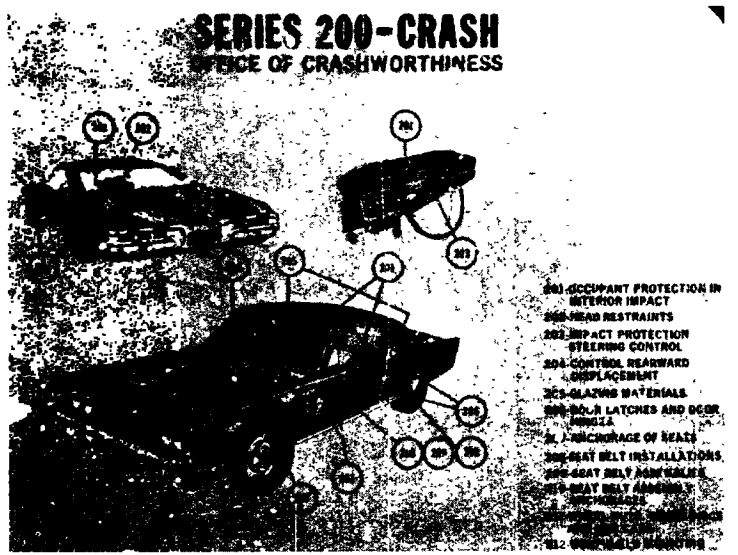


FIGURE 12

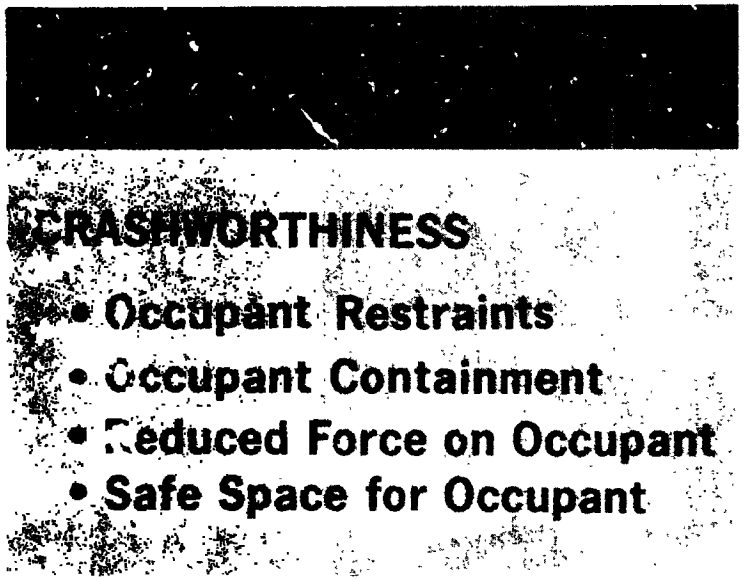


FIGURE 9

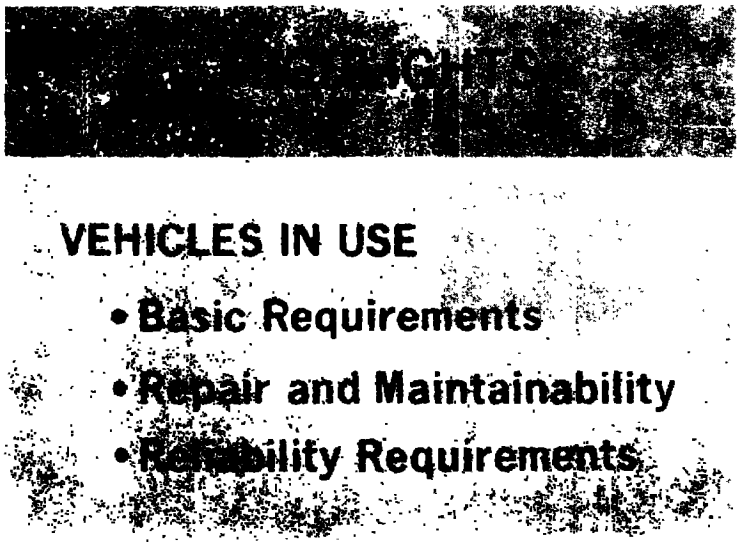


FIGURE 10

FIGURE 15

FIGURE 13

FIGURE 14

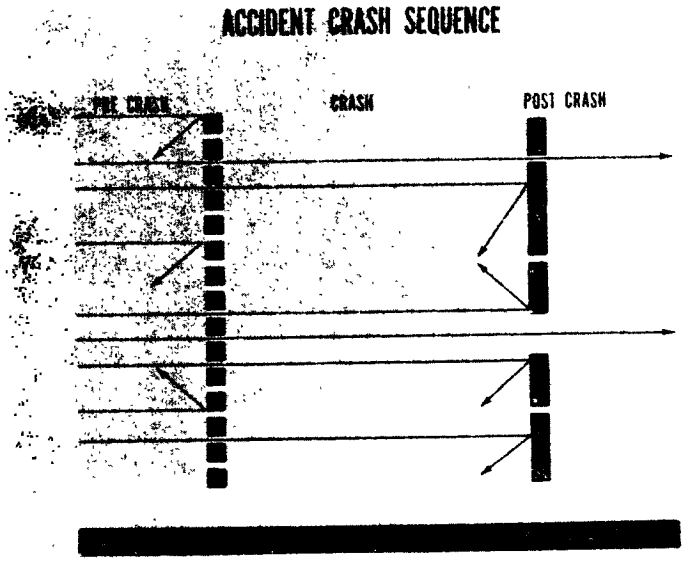
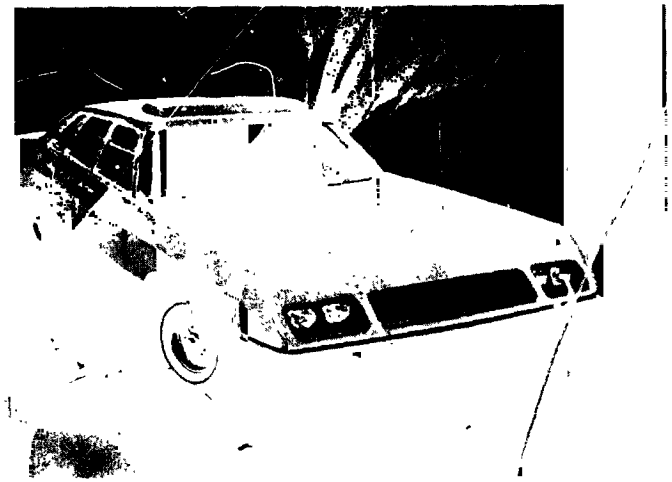
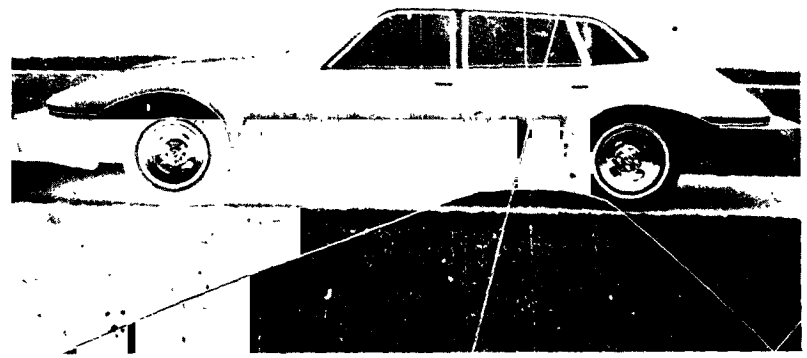


FIGURE 16





N72-25985

INTEGRATING A MULTIFACETED SYSTEM SAFETY PROGRAM FOR A LARGE COMPLEX SYSTEM

By

Mr. W. W. Malasky
Manager
Assurance Engineering
Litton Systems, Inc.

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

Man's concern with safety dates back to earliest pre-historic times, when his primary objective was survival against his enemies and the elements. However, as is the case with many other disciplines, the greatest advances made in System Safety have occurred in recent times. In the main, these advances have come about through efforts focused upon two classes of activity. One engaged in by relatively few people but of great interest to the general public, relates to man's recent extensions of his travels into new and unfamiliar environments - into the depths of the ocean, through the atmosphere at great heights and speeds, into outer space and onto the surface of the moon. The other interfaces with larger numbers of people and is concerned with the prevention of hazardous events that are potentially catastrophic to many, such as inadvertent nuclear explosion, of either a military device or a commercial power generating station, or loss of a large passenger aircraft.

The areas of System Safety Technology which have benefited the most as a result of these recent advances are:

1. The development of techniques for the identification of inherent problems so that all hazards associated with a given undertaking can be determined. This aspect of System safety Technology is discussed only peripherally in this document.
2. The formalizing of interfaces between System Safety and other technologies. This aspect will be dealt with at some length.

The need for such formalization in a large, complex system can be illustrated by considering a large ship such as LHA. This ship has many of the qualities associated with a city in that large numbers of people work, are housed, engage in recreational pursuits, are fed and are tended to medically. It has the qualities of an industrial complex by virtue of the various shops it contains. It has many of the problems usually associated with military operations, such as armament activity, storage of large quantities of combustibles and the need to conduct aircraft operations during good and inclement weather conditions. Finally, safety interfaces that relate to ecology and pollution must now be considered in a more formal fashion. In relation to this latter interface it can be considered that the ironclad rule usually accorded to ships' captains is now being challenged as a consequence of the pre-dawn collision between two oil tankers that occurred on 18 January 1971 which spilled nearly 900,000 gallons of oil into the ecologically sensitive San Francisco Bay.

INTERFACE WITH SYSTEM EFFECTIVENESS

The disciplines that conventionally relate most intimately to System Safety are Reliability (R), Maintainability (M), Quality Assurance (Q), Human Factors (H), and Value Engineering (V). Unification of these, and other, disciplines with System Safety can be achieved through various techniques. The one chosen for use in this presentation is system effectiveness, E, which is defined as

> The measure of the extent to which a system may be expected to achieve a set of stated system objectives.

In general form the functional relationship between E and the "ilities" listed can be written.

$$E(t) = f\left[\left(\frac{S}{\frac{a}{S_s}}\right), \left(\frac{R}{\frac{a}{R_s}}\right), \left(\frac{M}{\frac{a}{M_s}}\right), \left(\frac{Q}{\frac{a}{Q_s}}\right), \left(\frac{H}{\frac{a}{H_s}}\right), \left(\frac{V}{\frac{a}{V_s}}\right)\right] \qquad 1$$

since E is a function of t, and where

a is the achieved level of each parameter at some specified time in the system's life, and

s is the specified level established for that parameter.

The functional relationship expressed by equation (1) needs to be written as an explicit expression if a value of E is to be obtained at some point in time. However, no single explicit expression can be proposed, for E(t) depends upon factors that are unique to each system.

$$E(t) = f\left[\left(\frac{S_a}{S_s}\right)^{k_1}, \left(\frac{R_a}{R_s}\right)^{k_2}, \left(\frac{M_a}{M_s}\right)^{k_3}, \cdots\right] \qquad 2$$

$$0 \leq k_i \leq 1$$

Because of the considerable complexities in establishing and measuring the various parameters that comprise equation (2), it is necessary to obtain values for E by a process of optimization. This is discussed later.

INTERFACE WITH RELIABILITY

System Safety is more closely related to and allied with reliability than with any of the other disciplines defined by E. The basis for this strong interface becomes apparent upon examination of fundamental definitions. The generally accepted definition of Reliability is

> The probability that a system performs its intended function for a specified period of time under a set of specified conditions.

A definition for Safety that fits most requirements is

> Freedom from those conditions that can cause injury or death to personnel, damage to, or loss of, equipment or property.

Disregarding, for the moment, the fact that the definition for safety is qualitative rather than probabilistic in nature, it is evident that hazards which occur without causing injury or death to personnel, can fall into either the safety or reliability domain Further, it is also evident that injuries and fatalities can result from the inability of a system to perform its intended function, a reliability concern. Conversely, the occurrence of a hazard which affects only personnel, a safety concern, can, as a secondary effect, be responsible for preventing a system from performing its intended function, thereby degrading the reliability of the system.

One problem is brought about by the fact that the components of E are almost never completely independent of each other. Another relates to the fact that the components have different "utility values", k_i. When these are known, equation (1) can be written.

In order to define an interface between safety and reliability which can be operated upon by conventional scientific methods, it is necessary that both domains be quantified using compatible units. In the safety domain quantification is accomplished by assigning probabilities to events and then combining these individual probabilities into an overall probability. In most general terms, all safety calculations are derivable from the expression

$$P(S) + P(F) = 1 \qquad 3$$

where

- S is the set of events that describe safe performance
- F is the set of events that describe unsafe performance
- P(S) and P(F) are probabilities of the occurrence of S and F respectively

Having transformed safety into probabilistic terms, mathematical operation is carried out through manipulation with sample points, sets and events. It is possible to represent the S and F sets by means of a Venn diagram such as the one shown in figure 1. In this figure, the rectangle, I, is presumed to contain a finite number of sample points. These define the safe event, S, the unsafe event, S, the reliable event, R, and the unreliable event, R. In turn, each of these four events consist of

a defined collection of sample points, and each is a subset that is wholly contained in the universe, I. The interface between safety and reliability is represented by the lined area found between the arc acb, the extension of the safety event into the reliability event, and the arc dbb, the extension of the reliability event into safety. Two implications, readily apparent from an examination of figure 1 are:

1. R, the unreliable event, which is represented by all of the area outside the R event, includes sample points that are in the safe event.
2. Similarly, S, the unsafe event, represented by all the area outside S, includes sample points that are contained in R.

It might be presumed from an examination of figure 1 that the common goal of both safety and reliability is to expand the intersection of S and R, $S \cap R$, until $S \cap R = I$. This would be valid goal under the circumstance that I is comprised only of events in S and R. Complications arise when events and other disciplines must be included in I.

INTERFACE WITH RELIABILITY AND MAINTAINABILITY

Suppose now that maintainability considerations, which are also closely allied with the safety domain, are now inserted in I as shown in Figure 2. Maintainability is a characteristic of System Design, installation and operations which may be defined, for both hardware and human systems as

> The probability that the system will be retained in, or restored to, a specified condition within a given period of time, presuming that maintenance is performed in accordance with a set of prescribed procedures and allocated resources.

In turn, the term maintenance may be defined as

> All actions necessary for retaining this system or restoring it to a specified condition.

Since this definition of Maintainability is already expressed as a probability, its interface with Safety and Reliability can be expressed by means of a Venn diagram. In this, Figure 2, all the relationships between S, R and their compliments are the same as in Figure 1. The interface between M and S is represented in Figure 2 by the arc cdf, and the interface between M and R is represented by the arc ecs. The area common to all three events, S R M, is represented by the cross-hatched area bounded by the arcs c, cd and db. Perhaps the most obvious relationship observable from Figure 2 is that not all the sample points in the subset $M \cap R$ relate to the S event. This is due to the fact that the fundamental role of maintainability is to increase system life, without necessarily enhancing safety. As a consequence, the utility of maintainability to the system, reflected by the value of E, is enhanced as:

1. It becomes more expensive to replace the system rather than to keep it maintained.
2. Achieving longer system life through improved reliability or redundancy of parts becomes less cost effective than carrying out maintenance activities.

Consider now the safe event in relation to the R and M events shown in Figure 2. Let the sample points in S be divided into two subsets, one relating only to equipment damage, S_E, and one relating only to personnel injury, S_P. It is clear that S_P can occur even when S_E does not. For example, consider the case in which the life support system of a submarine is damaged during submerged operations. Presuming that a monitor and alarm system exists and that it can provide adequate warning time, there can be various sample points in S_P that may be selected such that the safe event can nevertheless occur.

Some sample points, in the area defined by $S \cap M$, presume that maintenance is possible, while others, in $S \cap R$, presume that the equipment to be used for contingency, escape or rescue is reliable. The following guidelines are offered in assigning sample points to $S \cap M$, $S \cap R$ or $S \cap R \cap M$.

1. Direct removal and replacement of faulty equipment, or the repair by personnel in situ, is contained in $S \cap M$.
2. Switching to a redundant equipment through remote means such as telemetry or in situ by attending personnel, is contained in $S \cap M$.

3. Switching to redundant equipment through the use of built-in, self checking circuits is contained in S∩M∩R.
4. Redundancy used in majority voting, for use in a fail safe configuration for replicated elements is contained in S∩R.

The process of idealizing the interrelationship described by Figure 1 involved an expansion by R and S sample points in I such that S∩R I. Although, in Figure 2, there are sample points located both in M and in R which permit the event S to occur, this process of idealizing can be extended to R∩S∩M by permitting the union of either R or M to fill the universe. That is,

$$(S \cap R) \cup (S \cap M) = I$$

It is clear that, even when there are as far as three variables, there will be advantages and disadvantages to selecting one of the two possible intersections for expansion in I. Increasing the number of variables that interact within I emphasizes still further the need for increasing the intersection of S with other parameters through the process of optimization.

SYSTEMS SAFETY IMPLIES OPTIMIZATION

It has been noted that the application of scientific methodology to safety requires the ability to quantify. Further, it is considered that scientific methodology applied to system safety implies optimization. To offer evidence for this point of view consider first the meaning of the term System Safety. First, a system may be defined as

> A device, scheme or procedure which behaves in accordance with some description, its function being to operate on information and/or energy and/or matter in some time reference in order to yield information and/or energy and/or matter.

This definition places no restriction upon the size or complexity of the device, scheme or procedure under consideration. Large systems such as the LHA, are usually comprised of some composite of operational and support equipment, personnel, facilities and software which are used together as an entity to perform or support a specified role. The operational role for a function performed by a given system is often referred to as its "mission". A system may be described by specifying

1. Its inputs and outputs as function of time.
2. All the possible conditions (states) of the system; i.e., the system phase space.
3. A descriptive model relating inputs, outputs, and system space as a function of time.

System inputs for LHA includes, among hundreds of others, operational plans, contingency operational plans, qualification and training requirements of crew members, maintenance and overhaul activities and a description of weather conditions. The system model includes considerations such as the rate of fuel consumption as a function of speed and range as a function of pitch and roll and alternate modes of operation in response to potential hardware and personnel problems. A definition for System Safety which relates all necessary factors is

> An optimum degree of safety, established within the constraints of operational effectiveness, time, cost and other applicable interfaces to safety, that is achievable throughout the life cycle of the system.

This definition does not imply that one, unique optimum is appropriate for the life of a system, although this possibility is not unacceptable. Rather, the definition establishes a requirement that sytems analysis techniques be applied to the domain of safety, and that these techniques include a quantification of safety over the entire life of the system based upon all facets of the system. As such, optimization is the essence of System Safety. It may be defined as

> The application of mathematics and simulation techniques for identification, examination and calibration of the interaction between and among the elements of the system.

OPTIMIZING SYSTEM SAFETY

Achieving an "optimum degree of safety" requires that choices be made among the various alternative means available for arriving at a chosen objective. Various "alternative

means" may be found within the domains of those disciplines defined by E or wholly within the domain of safety. This latter circumstance is illustrated by Figure 3 and is taken from the domain of hazard analysis. On the left hand side are the kinds of hazard analyses that are performed, generally successively in time, on a large system. On the right are shown the logical flow of hazard analysis outputs as a function of time. At one extreme, at t=0, are those tasks which imply the prevention of hazardous occurrences, and at the other extreme are those safety activities which are intended to minimize the effects of a hazardous occurrence. Although included for completeness, the tradeoffs between alternative means in one discipline are not as difficult as the selection of trade-offs among differing disciplines. Examples of alternate means which could be selected as optimum between various disciplines include configurations:

1. Of minimum complicity, as such that minimum demands are placed upon human skills for operation or maintenance.
2. Such that the failure of any one component can not lead to failure of the system or to personnel fatality.
3. Which provide an indication of those components that have become degraded and, consequently, are likely to fail.

It is apparent that no intelligent evaluation of alternative means can be made without relating to system objectives. If the domain of human safety is not involved, there is no hesitancy in permitting the system output to range over the domain of all possibilities in order to establish an optimum. System safety, however, is not free to trade-off all possible variations in system output. Specifically, it is considered undesirable in our culture to equate the value of human life in terms as inanimate equipment or money. Similarly, the notion that risks may be intentionally taken as part of the operation of a non-military system, based upon a schedule of compensation for injury or fatalities that may occur is equally undesirable in our culture. The suggestion that such an attitude is not rigorously pursued has, particularly in recent times, brought about confrontation between various elements of our society and the creation of a host of new industry and government agencies oriented towards resolving these differences. System safety cannot help but find itself at the focus of such considerations, and can make a valid contribution toward enhancing safety in our society through techniques that are useful for integrating multi-faceted programs for large, complex systems.

REFERENCES

J. E. Bylin, When Ships Don't Pass in the Night, The Wall Street Journal, 9 March 1971

S. W. Malasky, System Safety, Sparten Books (publication date to be announced)

J. F. McCloskey, and F. N. Trefethen, Operations Research for Management John Hopkins Press, 1956

F. E. Hohn, Applied Boolean Algebra, McMillian Company, 1960

R. M. Wilmotte, The Management and the Risk, IEEE Spectrum, April 1971, pp. 31-35

S. W. Malasky, Value Engineering Aspects of Safety in Manned Space Programs, Journal of Value Engineering, May 1966

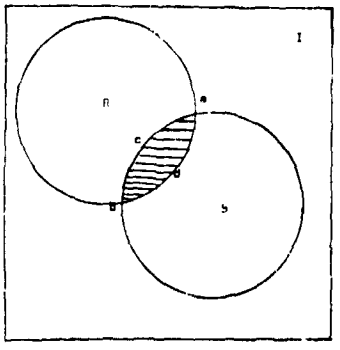
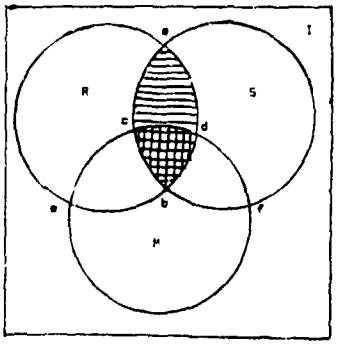


Figure 1 Reliability-Safety Venn Diagram



Reliability-Safety-Maintainability Venn Diagram

FIGURE 1

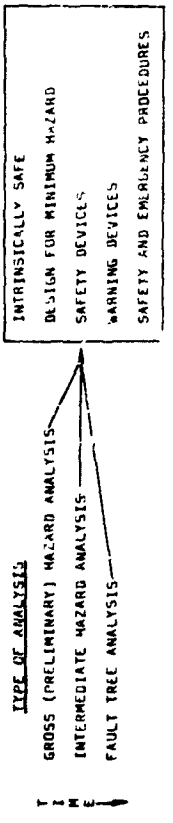


FIGURE 2

RELIABILITY TECHNIQUES
IN
THE PETROLEUM INDUSTRY

By

Mr. Henry L. Williams
Chief
CFE Engineering Branch
of
Reliability Division

NASA
Manned Spacecraft Center

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

Every taxpayer has an investment in the U.S. space program. A complete list of the many returns from U.S. manned and unmanned space programs would not be appropriate for this paper; however, the following examples are cited as being indicative of the number of benefits that have been obtained. In terms of domestic impact, the returns range from national pride to better paints. Early warnings of hurricanes discovered by satellites have saved lives and millions of dollars in property damage. The development of rechargeable batteries, stimulated by the space program, has brought remarkable changes in the design and use of portable power tools and appliances.

In addition to the domestic impact, the space program has also provided technology applicable to many industrial processes. Fireproof Beta cloth has been developed and is already being used for fire-fighter suits in municipal departments and on board aircraft carriers. The requirements for deep-space operations demanded major improvements in the state of the art of computer technology. The chemical industry is already using these advanced computers in large data centers.

The rigorous efficiency and performance requirements of the space age led to the development of new technologies for achieving the required reliability in the millions of complex components in space equipment. These rigorous requirements are particularly true for the Apollo spacecraft with its complex mission of taking men to the moon, landing them, and returning them safely to earth. The NASA Manned Spacecraft Center (MSC) at Houston, Texas, has responsibility for the development of the command module, the service module, and the lunar module. At MSC, the reliability and quality assurance organization is at the highest level within the center, and the Director of Reliability and Quality Assurance reports to the center Director. It is a basic philosophy within the center that reliability and quality assurance personnel have direct access to top management for resolution of problems. Reliability and quality assurance activities are so closely related that some activities can be classified as either reliability or quality assurance. Some of the reliability activities described in this paper may be considered re quality assurance tasks, as in fact they are elsewhere in NASA. If some reliability concepts appear to be missing, it is because they have been classified at MSC as quality assurance activities. Since the Apollo spacecraft constantly evolves to accommodate changing mission requirements, the reliability analysis of each spacecraft is affected. That is, the prohibitive cost of reliability demonstration, coupled with limited production runs, has caused NASA to emphasize a qualitative rather than quantitative analysis approach to reliability. Quantitative reliability evaluation depends on statistical information that requires large sample sizes such as those experienced in the automobile and chemical industries. This characteristic in the Apollo Spacecraft Program is precluded by the limited production. These qualitative techniques applied in achieving Apollo goals also have application to the chemical industry. Effective translation of this technology to the chemical industry requires that special attention be given to differences in (1) industry definitions, terms, and acronyms; (2) industry goals and motivations such as performance, cost, schedules, and safety; and (3) repeatability of product or process. The technological advances in reliability are concerned particularly with offsetting reliability demonstration costs and limited production runs.

Part I of this paper describes the qualitative disciplines, the definitions and criteria that accompany the disciplines, and the generic application of the disciplines to the chemical industry. Part II translates the disciplines into proposed definitions and criteria for the chemical industry, into a base-line reliability plan that includes these disciplines, and into application notes to aid in adapting the base-line plan to a specific plan or operation.

PART I - APOLLO SPACECRAFT RELIABILITY PROGRAM ELEMENTS

The basic objective of the Apollo Spacecraft Reliability Program was the development of a spacecraft that would safely carry man to the surface of the moon and back. The Apollo Spacecraft Program Manager and the Design Engineers were committed to this objective, which was reached by strict attention to details throughout the Apollo Spacecraft Program.

To accomplish this basic objective, the Apollo Spacecraft Program Manager was required to emphasize qualitative goals such as the following: (1) safe transport of man to the moon and back, (2) minimization of critical single-point failures, and (3) development of a spacecraft system that could be launched into earth orbit by a Saturn launch vehicle. These goals were attained through the imposition of reliability requirements on all three phases - design, manufacturing, and operations - of the Apollo Spacecraft Program. Attention to detail is achieved through the accomplishment of the following 10 disciplines, which will be discussed further:

1. Program management
2. Failure mode and effect analysis
3. Problem reporting and corrective action
4. Design specification review
5. Design review
6. Quantitative reliability analysis
7. Reliability test requirements
8. Maintainability
9. The parts program
10. Reliability documentation

These disciplines constitute a reliability program with the fundamental purpose of identifying and removing problem-causing elements from the design and, ultimately, from the equipment selected to implement the design. This approach to identification and removal of problem elements is summarized in Figure 1.

Program Management

Basic NASA reliability requirements are contained in the NASA reliability publication NPC 250-1, entitled "Reliability Program Provisions for Space System Contractors," July 1963. These requirements are further defined and modified for use at MSC by MSC document MSCM 5315, entitled "Supplemental Reliability Requirements and Implementation Instructions for Manned Spacecraft Center Equipment," May 1969. These documents provide the basis for the Apollo Spacecraft Reliability Program, which is implemented primarily by the contractors that have responsibility for major hardware elements. Management of the reliability portion of a contract is the responsibility of the Reliability Division of the Reliability and Quality Assurance Office at MSC.

Reliability provisions in contracts and supporting reliability program plans are the primary tools of reliability program management. Each contractor develops a reliability program plan to detail how the provisions of the contract will be implemented. This plan, which is reviewed and approved by MSC, establishes the scope, applicability, and organizational responsibilities of the contract. The development of each contractor's or each subcontractor's program plan is guided by the Reliability Division, which considers factors such as the following: (1) the complexity of the equipment, (2) the functional criticality of the equipment, and (3) the procurement size. In the plan, the 10 reliability tasks previously discussed are described in terms of their basic requirements, definitions, implementation, procedures, exceptions, and data generation. The plan also establishes guidelines for scheduling the analyses, reporting the results, and distributing the necessary information to user agencies.

The Reliability Division continuously monitors the contractor's progress and conducts periodic meetings with the contractor to resolve implementation and scheduling problems. These meetings are based on the continuous interactions of the two organizations and on periodic formal audits of the contractor's performance with respect to the program plan requirements. The Reliability Division of MSC also places requirements on the contractor concerning the management of subcontractors and the reliability data to be generated by the subcontractors. Personnel from MSC may participate periodically with the contractor in his audit of the subcontractor.

The application of the Apollo Spacecraft Reliability Program concept to the chemical industry consists of developing a plan (1) that establishes division or corporate policy on reliability requirements such as (a) reporting failures and (b) criteria for accepting new equipment from vendors and (2) that establishes reliability requirements for turnkey plant design and construction.

Failure Mode and Effect Analysis

A designer usually evaluates his design by a thought process in which he examines possible

5-5

failure mechanisms, and protection for the failure mechanisms thus identified is provided. In the Apollo Spacecraft Reliability Program, this mental exercise is documented, put into a logic format, and complemented with the "what if" logic of the test, operations, and reliability engineers. This documentation affords the designer an evaluation of the design concept in which the complete set of requirements for the equipment is considered. This analysis is known as the Failure Mode and Effect Analysis. Inputs to the analysis include a description of the function the equipment is to perform and historical performance data on similar equipment. The analysis is oriented toward discussion of how items will fail rather than of how to make them work. The analysis consists of (1) an examination of each component of the system or function and (2) identification of the modes in which each component could fail. The effect component failure has on the system or function is then determined. Where interrelated functions exist, it is also necessary to evaluate the effect the failure has on other elements of the equipment. The failure effects are evaluated against established criticality definitions, with attention focused on major problems requiring design modification or procedural workarounds. Equipment (such as power, air conditioning, and structural support) that has service functions is included in the analysis.

The criticality definition for the Apollo Spacecraft Program had three categories: (1) personnel safety, (2) mission termination, and (3) all others. For the chemical industry, this definition is translated directly to (1) life/property loss, (2) plant shutdown/product contamination or loss, and (3) all others. When the selected set of definitions is used, the analysis provides a list of equipment elements whose failure could cause an undersired event. In the Apollo Spacecraft Program, these elements are referred to as single-failure points, which implies that the list does not contain combinations of failure points which could cause an undesired event. This list of equipment elements is the basis for a management function to force either redesign of these elements, provision of a workaround to offset the failure of these elements, or location of a different way to perform the function. In cases where no corrective action is available for a single-failure point, program management approves launch commitments after assessment of remaining risks.

The discussion up to this point has been focused on design activity. The Failure Mode and Effect Analysis is used in other ways such as to provide an input to the test requirements by identifying elements that require functional acceptance testing. Inputs are provided to the prelaunch checklist by identifying backup elements and workarounds which should be verified. The Failure Mode and Effect Analysis also serves as a working tool for the operations engineer by providing him with an aid in fault isolation. The Failure Mode and Effect Analysis is a design tool which has application throughout the life cycle of the equipment.

Figure 2 presents an example of the Failure Mode and Effect Analysis format used at MSC. The format in Figure 2 is simpler than the one actually used for the spacecraft, but is a good example for illustration purposes. The Failure Mode and Effect Analysis format might might be used in the chemical industry in the following ways:

1. As a joint analysis performed by plant designer and customer to check the design concept against the operating procedures to be used.
2. As an analysis performed as a design tool and then charted in summary form as a fault isolation aid during startup.
3. As an analysis performed as an aid in selecting instrument points for supervisory control of a plant or process.

The Failure Mode and Effect Analysis is considered to be a major factor in achieving trouble-free performance. This analysis is particularly useful where complex operations with interrelated functions required design detail by serveral designers.

The single-failure-point list resulting from the Failure Mode and Effect Analysis provides the designer with an action-item list of problems to be solved. When documented for the final design, the Failure Mode and Effect Analysis traces the effects back to the causes.

Problem Reporting and Corrective Action

Many unscheduled repairs, equipment failures, and catastrophic losses are avoidable if constant attention is given to prevention of their occurrence. Recurrence of a problem can

be avoided if effective corrective action is taken the first time the problem occurs. Recurrence control depends on communication among all users of the problem-causing equipment. A problem-reporting and corrective-action system is used by NASA in the Apollo Spacecraft Program Program to report problems, monitor the application of corrective action, and implement recurrence control.

Using a carefully selected problem definition, personnel concerned with the life cycle of a piece of equipment report the occurrence of any problems. These problems are recorded in a permanent record for that piece of equipment. Each reported problem is checked for previous occurrence and for the adequacy of previous corrective action. A solution must be found for all reported problems; that is corrective action must be identified and implemented. The corrective action must be based on a sound engineering solution to the problem. Failure analysis is the basis for the solution and may range from simple inspection of the failed equipment to special tests that duplicate the conditions of failure. Sufficient engineering effort is applied to clearly identify the cause and to understand the conditions which influence failure occurrence. The organization responsible for the reporting system verifies the corrective action before the problem is officially considered to be solved. This problem-reporting and corrective-action system prevents inferior elements or concepts from reaching the operational status. Also, when used along with the Failure Mode and Effect Analysis, this system provides a dual approach to reducing the occurrence of problems throughout the life cycle of the equipment.

The important elements of problem reporting are (1) the basic problem definition, (2) the basic critical-function definition (should be the same as the Failure Mode and Effect Analysis), (3) effective reporting techniques, (4) well-planned corrective action, and (5) careful correlation of the recurrence control history.

The application of the problem-reporting and corrective-action system to the chemical industry can be related to the development of new equipment and to the distribution of problem histories to other plants and divisions within the user company. If a valve jams in the open position and cannot be closed, all other plants in the organization should be notified if they are using the same valve in the same application. If a minor problem occurs when an engine is in a noncritical application, an audit can be made to determine if the engine is used elsewhere in a more critical function and whether corrective action is necessary. This system can also be used (1) to provide inputs to inventory control systems, (2) in maintenance planning, and (3) in the support of unit turnarounds. In addition, this system can be used by management to maintain an overview of program problems and their status.

Design Specification Review

Reliability considerations should form an integral part of the preparation, review, and approval of all design specifications, vendor-change requests, specification drawings, purchase orders, and subsequent revisions or amendments or both. A design specification is not adequate until the reliability requirements are clear to the designer. The reliability requirements include qualitative reliability goals, reliability procurement goals, and reliability documents goals. The same requirements must also be applied to vendor-deviation requests. This approach to design specification review is directly applicable to the chemical industry.

Design Review

The entire reliability program represents a continuous design review effort. From conceptual configuration studies to eventual design freeze, reliability continually evaluates the systems and updates analyses. Design reviews are conducted at the following hardware levels: (1) component, (2) subsystem, and (3) system. Each contractor has his own method of conducting design reviews, but participation by representatives of all disciplines (such as engineering, quality, reliability, manufacturing, and purchasing) is required. Some of the primary purposes of the design review are to determine the following: (1) Have all potential failure mechanisms been eliminated? (2) Is the item manufacturable? (3) Can the item be inspected? (4) When put together as a subsystem or system, will all components work together as specified?

Reliability personnel have a prime role to play in the major system design reviews, which are the Preliminary Requirements Review where the spacecraft requirements are established; the Preliminary Design Review where the conceptual design is reviewed and approved; the Critical Design Review where final design approval, along with the go ahead for the manufacturing phase, is granted; and the Flight Readiness Review where approval for launch is given after a review of all data associated with the spacecraft. Table I correlates the system design reviews to equivalent events in the development of a chemical process.

Quantitative Reliability Analysis

The Apollo Spacecraft Reliability Program consists primarily of qualitative disciplines. As stated previously, limited production quantities, extremely high reliability requirements, and evolutionary changes to the spacecraft preclude the use of statistical inference to assess the numerical reliability of the spacecraft. Reliability predictions using historical data of similar equipment have been accomplished for the purpose of comparing alternate approaches. These design studies that have a common historical base are valuable for comparison of different configurations of equipment selected from the data base.

Differences among the equipment in the data base and the actual Apollo hardware preclude accurate predictions of the total spacecraft reliability. However, statistical analysis of test results, performance parameters, and physical properties are performed by other organizations.

Reliability Test Requirements

The reliability organization functions as an integral part of the contractor's test program and is required to ensure, through analysis and proof, that all equipment will perform to the design intent. The reliability organization concurs in all test plans, specifications, and reports. The responsibility of the reliability organization is to evaluate all performance aspects to ensure that all parameters (thermal, vibration, environment stress, etc.) are properly applied and that the results demonstrate the design competence.

Test planning and monitoring are continuous disciplines covering programs on design concept, design verification, prototypes, thermal or environmental (or both) conditions, qualification or certification (or both), acceptance, parts and materials, subsystems, systems, and end-items. Each program requires unique analysis and evaluation to ensure prompt correction to design concepts for a progressive evolution to product reliability. Special emphasis is placed on monitoring the qualification test program which tests the equipment in the actual usage environment including vibration and thermal conditions.

In development and qualification tests, the objectives are related to verification of the design approach. During acceptance test and checkout, the emphasis shifts to verification of the manufacture and assembly of the equipment. Reliability supports these activities with design information and test histories.

Maintainability

The Apollo spacecraft was designed with standby and redundant systems to free the crew from inflight maintenance tasks which might interfere with critical crew functions. Maintainability for the spacecraft consists primarily of fault isolation and switching to backup systems. Because of the need to control the operating time which accumulates on certain equipment prior to launch, equipment with limited operating life time is identified and carefully monitored during ground tests and checkout. If insufficient operating lifetime remains, the equipment is replaced prior to launch. The Failure Mode and Effect Analysis, which was discussed previously, provides inputs to the ground-support-equipment maintenance program by identifying critical equipment for which rapid repair or replacement is required during launch operations.

Parts Program

The NASA reliability publication NPC 250-1 establishes parts criteria for space system contractors. This document requires contractors to implement a program covering selection, specification, qualification, and application reviews of parts for all items to be used in a system. A parts program plan

must also be submitted as part of the reliability program plan. By review and approval of the plan, NASA assures that an acceptable parts control program is implemented by Apollo contractors. The elements of an acceptable control program include qualification, lot acceptance, parts screening and burn-in, and derating.

When departures from program criteria are identified, a detailed technical review of the critical part applications is accomplished to ensure that an adequate rationale for such usage is provided. The assessment activities also include the evaluation of part failures in equipment, the corrective action taken, and an evaluation of the possible impact of problems reported by the NASA ALERT system and other sources. The NASA ALERT system is a program which requires that all NASA installations exchange information on significant parts and materials quality or application problems of general concern. A computerized parts master file provides the identification and applications of all spacecraft electrical, electronic, or electromechanical part. The use of this file permits a rapid evaluation of the potential impact of a problem with any given part type. Significant electrical, electronic, and electromechanical part problems receive particular program management attention. Effective resolution and closeout are verified progressively at major milestone reviews.

The Apollo parts program has concentrated on electrical, electronic, and electromechanical parts because of their predominance in the space program. The program outlined previously was based on acceptance of each part. The high design margin of mechanical parts used predominantly in the chemical industry suggests a program which emphasizes the rejection of bad parts. This control can be accomplished through a system similar to the NASA ALERT program.

Reliability Documentation

The quantity of documentation of the Apollo Program is very large. Yet, the complete, clear story that can be retrieved concerning problem history and equipment tests serves a purpose in such an immense program as Apollo, with approximately 40,000 companies involved in the program. Clear, concise information concerning results from reliability activities is necessary, and a level of documentation to support this requirement is necessary. Documentation requirements adjust as the associated program evolves from its design conceptual phases through design maturity and product operational phases. The necessity for accuracy and technical excellence is obvious when the impact on crew safety or mission success is considered. Reliability design analysis is made available for use by operational personnel in a large program or company only through documentation.

PART II - APPLICATION TO CHEMICAL INDUSTRY

Introduction

With careful attention to economic factors, the techniques discussed in Part I can be applied successfully to the chemical industry. This paper describes the qualitative program elements which are the basis of the Apollo Spacecraft Reliability Program. The application of the techniques to the chemical industry requires careful attention to economic feasibility. Failure Mode and Effect Analysis and problem reporting are the basis for a sound qualitative reliability program in the chemical industry.

The high reliability of the Apollo spacecraft is a demonstration of the effectiveness of qualitative reliability requirements. On the Apollo 8 mission, only five of 5,000,000 parts failed to perform their function. If a level of 99.9 percent had been achieved for the reliability of these parts, then one part in a thousand might be expected to fail. Thus, on each flight, approximately 5,000 parts could be expected to fail.

Reliability Program Implementation

The reliability program elements described previously have been effectively applied to large and small procurements. Procurement size influences the associated reliability plan in two ways. Most smaller procurements are accomplished by a prime contractor on a subcontract basis. The reliability program of the

prime contractor is extended to cover the subcontracted equipment. In other small procurements, the function of the equipment may be completely noncritical to the mission objectives. In this case, minimal reliability requirements are implemented.

For all procurements for the Apollo spacecraft, the definitions "loss of life" and "mission termination" are used to judge the criticality of the function. For the chemical industry, it may be necessary to use a variable definition of critical function. For example, an automatically controlled process which has a throughput capability in excess of demand is not sensitive for loss of life or of productive time. But, the process may have an economic hazard of much consequence such as contamination of a catalyst, spillage of an expensive feedstock, or destruction of property. Although this example oversimplifies safety considerations, it is obvious that variability of definitions is necessary. The following are the major factors which influence the degree of implementation of a reliability program for a given plant or process.

1. Scope - Plant size, number of similar plants, procurement size
2. Contract tier - Turnkey designer, equipment supplier, volume component supplier
3. Criticality of function - Obvious critical functions, unknown or obvious lack of critical functions
4. Definition of criticality - Safety, facility loss, production schedules, economics

The following are the steps in implementing an effective reliability program utilizing the Apollo disciplines:

1. Use the disciplines previously described to structure the basic reliability requirements for a plant, division, or corporation. More extensive commitment to the basic requirements means more success in the individual applications. The basic requirement should include a definition of problem and definition of criticality categories coordinated with the intended users.

2. Perform the following for each segment of the organization, plant, or process:

a. Extend or subdivide the definitions of problem and criticality to fit special conditions. Definitions need not be changed, only supplemented.

b. Examine each reliability requirement in terms of the implementation factors (scope, contract tier, criticality of the function, and criticality definitions). Judge the effectiveness of the requirement in supporting overall objectives (schedules, minimum nonproductive time, reduction, effective turnarounds, and product quality).

c. Develop a procedure for each basic reliability requirement which is economically feasible when the factors in items a and b are also considered.

d. Document the procedures in item c as a plant reliability plan.

e. Develop the forms, data flow, and signature approvals to support the plan.

f. Implement the plan, and train personnel. (The importance of proper training in reliability requires careful planning for this step.)

Implementation for Equipment Suppliers

Equipment suppliers should consider the elements of the baseline plan in development of new product lines. However, the Failure Mode and Effect Analysis and design specification review techniques can strengthen the sales brochure or application guides. Documenting the results of environmental tests and other demonstrations of specification requirements aid the customer in his design review. The Failure Mode and Effect Analysis can be used to define configurations of instrumentation power sources and physical position which offset potential failure modes. This acknowledgment of possible failure modes does not detract from the qualifications of the equipment to the customer who is reliability oriented.

Implementation for Turnkey Design Companies

The base-line reliability plan can probably be most effectively adapted for use by an organization having total responsibility for development of a process facility. Reliability requirements can be implemented at the beginning of the project. The Failure Mode and Effect Analysis proves its value in the selection of the best equipment configuration. Problem report summaries provide an effective way of directing project management and

customer attention to the critical problems of the development cycle, and the customers feel less inclined to oversee the details of the project. An effective set of milestone reviews can be established in which the major problems and corrective actions are reviewed in detail and in which the majority of the project is reviewed in summary format. The problem-reporting system must be good enough to provide confidence that the important problems will stand out. The criticality categories sort all problems into tiers of importance, which allows effective audits of lower tiers. This procedure, which is "management by exception" in the basic form, requires dependence on accurate reporting of events.

Implementation for Startup and Operation

The qualitative approach to reliability as described in this paper focuses attention on designing reliability into a system. Requirements for replacement of limited-lifetime equipment and for preventive maintenance are translated into operational requirements. Problem reporting continues into the operational phase and becomes the focal point of operational reliability. Qualitative reliability documented analysis performed during the development program benefits this phase. The Failure Mode and Effect Analysis provides a basis for fault isolation diagnosis during startup and operations. Review of the Failure Mode and Effect Analysis and of corrective action for problems provides a list of items to be given special attention or checks prior to startup. These data also provide inputs to supervisory control instrumentation points and control functions. The later addition of equipment such as supervisory control to the process requires that the new equipment be subjected to the total requirements of the reliability plan.

Reliability Program Plan

Appendix A contains a base-line reliability program plan for a multiple-plant division or corporation. The plan defines requirements, including procurement of equipment or turnkey plants, for the total life cycle of plants within the division. Implementation of the plan for a division should be accomplished by coordination of the requirements with managers, operators, and engineers from each plant and by modification of the requirements until practical implementation is possible. The plan should then become official procedure, subject only to periodic review and update, as necessary for solving operational problems.

CONCLUSIONS

The reliability program at MSC is basically qualitative in nature, with major emphasis on the disciplines of problem reporting and corrective action and Failure Mode and Effect Analysis. This qualitative approach is most appropriately applied to complex, one-of-a-kind projects. Several chemical industry segments meet this criterion.

Success in implementation of this approach will depend on implementation of each discipline, using definitions and criteria derived separately for each application. Carefully planned and correctly scoped, a reliability program and increase profitability of many chemical operations through reduction of downtime, reduction of equipment losses, and reduction of contingent liability. Implementation of the reliability program for effective management and control is best accomplished by development of a program plan that has been coordinated with all organizational elements involved.

APPENDIX A

BASE-LINE RELIABILITY PROGRAM PLAN

INTRODUCTION

The purpose of this document is to set forth the basic reliability requirements for the_____Division of_____Chemical Company. Management directive _____ authorizes this document and necessitates implementation of the requirements for all processes put into operation after___(date)___. All processes put into operation prior to ___(date)_____must implement the requirements which have operational application. (See implementation guide, page____.) Requirements for safety, quality assurance, maintenance, and testing should be considered in implementing these requirements in order to avoid duplication of effort.

RELIABILITY REQUIREMENTS

The_____Division reliability program consists of the following activities which take place during the development and operation of processes.

Reliability Program Plans

A reliability program plan shall be developed for each plant or operation in this division. Each requirement shall be implemented by a plant procedure or operating rule. Any procedure or rule which conflicts with this plan must be approved by division management. Requirements shall be implemented to the extent appropriate for each of the following cagegories of equipment:

1. Equipment previously installed
2. Standard off-the-shelf equipment procured on a lot basis
3. Special procurements of major equipment items
4. Multiple equipment procurements (turnkey plants)

Design Specification Review

Each design specification shall be reviewed in order to accomplish a correlation between the design and the operating plan functional requirements. Each specification will be reviewed for performance requirements, safety, human factors, test criteria, maintainability, environmental requirements, and equipment that has a limited operating lifetime. The specification shall be reviewed against the basic operating plan and appropriate emergency and standby procedures.

Failure Mode and Effect Analysis

The Failure Mode and Effect Analysis shall be accomplished for each new process facility. The analysis shall identify possible failure modes, the effect on the process, and the criticality of the effect. A control list of the equipment which has Criticality I and II failure modes shall be established and shall be maintained as a major status document during the development of the process. The list shall contain the equipment name, the critical failure mode, the effect, and the proposed corrective action. A process cannot be put on line until all Criticality I failure modes have been eliminated and until all Criticality II items have adequate workarounds. The following are the criticality categories:

I. Destruction of life or process facility
II. Interruption of the process
III. All other critical factors

Problem Reporting and Corrective Action

A problem is defined as the failure of an equipment to perform its intended function when required. A problem may be caused by design inadequacy, quality defect, procedural error, or human error. Problems are categorized as Criticality I, Criticality II, or Criticality III. A system will be developed for reporting problems which occur in any equipment during or subsequent to acceptance testing. A list of Criticality I and II problems and the associated corrective actions will be established and maintained as a major status report during the development and operation of a process. Any problem on this list for which corrective action has not been taken is considered to be an open problem. A process will

not be put on line if any equipment has open problems. The following are other features of the system:

1. Reporting of open problems to management will be scheduled so that timely knowledge of risks will be provided.

2. Each problem reported will be correlated with the Failure Mode and Effect Analysis to determine the criticality category. If the problem has not been identified in the Failure Mode and Effect Analysis, the criticality category shall be identified through analysis, and the data shall be added to the Failure Mode and Effect Analysis.

3. Each problem report of a limited-lifetime item shall include the operating time at the time of failure.

Parts Program

Equipment with basic design proven inadequate for a process is defined as an ALERT item. Each item will be reported to the _____ Division headquarters for distribution to other plants. If Division headquarters receives an ALERT concerning lot-procured items, a procurement stoppage will result until the ALERT can be investigated. An ALERT report from a plant should include identification of the successful substitute.

Reliability Test Requirements

For test under the cognizance of this division, problems encountered during testing must be reported as defined in the section entitled "Problem Reporting and Corrective Action." Problems must be reported during and subsequent to acceptance testing for equipment which is intended for use in this division. If the test is conducted prior to transfer to this division, problem reporting requirements will be included in the specification or procurement document. The acceptance test for equipment to be assigned to this division must include a functional demonstration in the specified environments of pressure, temperature, atmosphere (salt water, etc.), vibration, and compatibility with process feedstocks and products for lot-procured items. Previously documented tests of three or more units satisfy this requirement.

TABLE I

CORRELATION OF INDUSTRY MILESTONES

AEROSPACE INDUSTRY MILESTONE	CHEMICAL INDUSTRY MILESTONE
PRELIMINARY REQUIREMENTS REVIEW	REVIEW OF PRELIMINARY SPECIFICATION
PRELIMINARY DESIGN REVIEW	MANAGEMENT APPROVAL TO RELEASE DESIGN SPECIFICATION
CRITICAL DESIGN REVIEW	MANAGEMENT APPROVAL TO RELEASE DRAWINGS TO MANUFACTURING
FLIGHT READINESS REVIEW	MANAGEMENT APPROVAL TO START UP PLANT

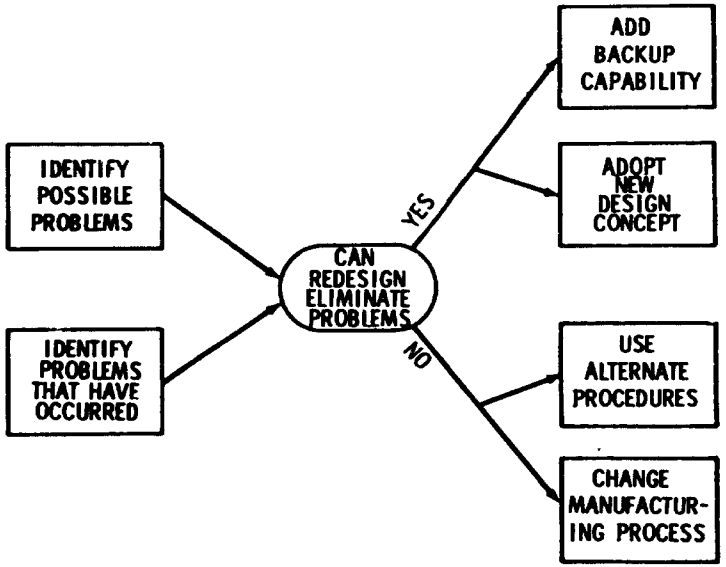


Fig. 1. Basic reliability approach.

ITEM IDENTIFICATION, FUNCTION, AND QUANTITY USED	FAILURE MODE	CRITICALITY	FAILURE EFFECT (a) MISSION (b) SPACECRAFT (c) SUBSYSTEM (d) RELATED SUBSYSTEM (e) INTERFACES	FAILURE DETECTABLE BY		ALTERNATE MEANS OF OPERATION	POTENTIAL HAZARDS RESULTING FROM FAILURE OR FAILURE PROPAGATION DURING CHECKOUT THROUGH RECOVERY	REMARKS OR RECOMMENDATIONS
				SC CREW	GROUND CREW			

FIGURE 2

N72-25987

SYSTEM SAFETY ENGINEERING IN THE DEVELOPMENT OF ADVANCED SURFACE TRANSPORTATION VEHICLES

Harry E. Arnzen
Grumman Aerospace Engineering Corporation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 197_

I. INTRODUCTION

This paper describes applications of System Safety Engineering to the development of advanced surface transportation vehicles. The concept of System Safety has matured with aerospace programs and is now contributing safety methodology to non-aerospace segments of our society. As a pertinent example, the paper describes a Safety Engineering effort "tailored" to the particular design and test requirements of the Tracked Air Cushion Research Vehicle (TACRV), developed by the Grumman Aerospace Corporation, under contract to the Department of Transportation. The test results obtained from this unique research vehicle, will provide significant design data directly applicable to the development of future tracked air cushion vehicles that will carry passengers in comfort and safety at speeds up to 300 miles per hour.

Part II of the paper summarizes the Safety Engineering efforts implemented during the TACRV design phases. A detailed outline of the significant safety provisions, incorporated during the design of TACRV, is included in Part III. The safety engineering effort applied during the design of the Tracked Air Cushion Research Vehicle reflects the experience gained from a wide range of operational systems designed and manufactured by the Grumman Aerospace Corporation. These include commercial and military aircraft, space vehicles, hydro-foils and an experimental scientific submersible. Incorporation of the appropriate features into the TACRV design provides the desired result of a safe research vehicle. Hazards to operating personnel have been reduced to a minimum.

Part IV of the paper describes System Program techniques and the analytical methodology that is applicable to public transportation systems of the future, derived as a "spin-off technology" from aerospace programs. Two typical tracked air cushion vehicles for future public transportation are illustrated in Part V and the related system safety objectives are highlighted.

II. TACRV SYSTEM SAFETY PROGRAM

- OBJECTIVES
- SCOPE
  DESIGN, MANUFACTURE AND TEST
- APPROACH AND METHODOLOGY
  DESIGN SAFETY CRITERIA AND GUIDELINES
  SAFETY REVIEWS
  DRAWING REVIEW AND SIGN-OFF
  SAFETY CONTROLS IN VENDOR SPECIFICATIONS
- MANUFACTURE PHASE MONITORING
- VEHICLE TEST CONSIDERATIONS

This part of the paper discusses the Safety Engineering Program implemented during the TACRV design and manufacturing phases, and reviews future test program considerations. The primary objective of this safety program has been to eliminate or reduce potential hazards associated with operation and maintenance of TACRV. Potentially catastrophic items were eliminated during early design. Critical hazards identified have been eliminated or reduced through use of safety devices, warning systems and/or precautionary procedures. In summary, the objectives of the program have been to establish requirements, procedures, and methods, to ensure personnel safety and minimum risk of damage, or degradation to equipment.

SCOPE OF PROGRAM

The scope of the TACRV Safety Program includes the active participation by Safety Engineers, design and systems personnel, in all phases of design. The significant program milestones and related system safety engineering tasks are illustrated in Figure 1. The Grumman approach to system safety is "the total integration of available skills and resources to achieve maximum safety assurance." Safety Program activities generated by this concept included:

- Performance of analytical studies to a practicable depth for hazard identification. These include preliminary (gross) hazard, hazardous failure-mode and systems integration studies on the vehicle, subsystems, crew station, wayside power and guideway/vehicle interfaces
- Participation of Safety Engineers at design reviews, safety reviews and informal inspections
- Recommendations for emergency systems, safety devices and/or emergency procedures, for identified potential hazards which cannot be eliminated
- Provide guidance and support to design personnel through development of safety design criteria and check lists "tailored" to the operating environment of TACRV

Many technical disciplines contributed to the safety assurance effort, including:

- Reliability/Maintainability - failure and maintenance studies.
- EMI - Safety inputs on vehicle grounding, internal bonding, dissipation of of electrostatic charges and lightning protection considerations.
- Power Plant - Crashworthy fuel system technology, thermal protection and combustion prevention considerations.
- Crew Systems Design - Human Factors aspects of Controls and Displays.
- System and Project Engineering; GAC System Safety Staff.

MANUFACTURE PHASE MONITORING

The system safety effort planned for the manufacturing phase of TACRV includes monitoring the vehicle assembly stages, equipment installation and systems checkouts. The purpose of this effort is to identify and correct any potentially hazardous interface conditions, between lines and equipments, that were not anticipated during the design phases. The safety engineer will make corrective action recommendations to the project engineer, whenever unsafe conditions are identified. In summary, the safety tasks will include the following:

- Observe acceptance tests of major equipments and propulsion systems, to verify compliance with safety requirements, before installation in the vehicle
- Monitor installation of all major systems and subsystems in order to identify potential ignition or combustion hazards, in each compartment, from possible leakage, chafing, and/or electrical shorts, due to close proximity of interfacing line connections or interference with vehicle structure
- Inspect turbofan engine installation to identify potentially hazardous conditions related to engine/vehicle integration. Examine engine control linkages for freedom of travel. Assure adequate thermal protection for equipments and lines in high temperature areas. Review all potential fluid leakage and drainage paths, in engine compartments
- Monitor installation and checkout of all emergency equipment (i.e., fire detection/suppression, caution/warning, etc.) and safety devices to verify failure-free operation
- Incorporate safety oriented requirements into each vendor specification and specification control drawing
- Conduct drawing review and sign-off on selected major installation drawings where safety provisions are involved
- Review of test plans, test reports and operating procedures to determine impact on safety. Review and evaluate precautionary procedures. Review all test failures for unanticipated hazardous conditions and recommend corrective action
- Develop a pre-accident plan for coordinated Grumman support in accident investigations
- During subsequent phases, System Safety will review all previous safety studies, develop operating and maintenance procedures and monitor vehicle test site operations

APPROACH AND METHODOLOGY

Although there are some differences in the Safety Engineering effort between Lunar Module, Military Aircraft, TACRV and similar advanced surface transportation systems, there are significant differences in the accident potential and the approach to practicable solutions to reduction or elimination of injury and damage to equipment. In addition, the level of risks that are acceptable in military and space operations are not acceptable in public transportation. This aspect is what we are ultimately dealing with, in our approach to achieving safety assurance.

In the absence of a formal system safety engineering standard, such as the military requirements of MIL-STD-882, ("System Safety Engineering Program for Systems and Associated Subsystems and Equipment; General Requirements for"), special attention was given to "tailoring" a system safety program to the specific needs of the TACRV Program. In lieu of costly and extensive systems safety analyses described in MIL-STD-882, all engineers and designers were provided with a "design safety criteria and guidelines" document, developed by the Safety Engineer, to enable all personnel to assist in hazard identification and elimination in the early phases of design. The majority of these "guidelines" has been previously established for use in the design of military and civil aircraft and spacecraft. The criteria were used continuously by design personnel as a check-off list during the vehicle and subsystems design.

Where critical hazards were identified, the Safety Engineer conducted accident and safety equipment research to review the "state-of-the-art" in safe system design and offer practicable recommendations. For example, TACRV has the combination of a large volume of JP-5 fuel for the turbofan with a 7000-volt LIM electrical propulsion system on board the

vehicle. Crew survival is now assured by incorporation of a crashworthy fuel tank and piping system. Another typical safety study involved evaluation of the required number, size and locations of doors and escape hatches to assure safe exit and/or rescue, under any conceivable mishap condition.

Drawing Review and Sign-Off

Drawing reviews were conducted during the early stages of systems and equipment design to identify and correct unanticipated hazards and to recommend appropriate emergency systems, fail-safe features and safety devices. Particular attention was given to review of critical systems that are employed during emergency situations. Typical examples of layouts and drawings reviewed for these systems and equipments included crew station, emergency controls, escape hatches, caution/warning, fire detection/suppression, vehicle grounding, brakes and fuel systems.

Effective control of design safety, for subcontractor supplied equipments, was established by incorporating safety oriented requirements into each Specification Control Drawing (SCD). Preliminary and final "SCD's" were reviewed to verify compliance, or make additions, to the safety requirements. These included such items as safety factors, leakage tests, proof tests, fail-safe and non-flammable requirements, where applicable. All "SCD's" required final sign-off by the Safety Manager.

Useful Inputs from Other Disciplines

Employment of the "Safety Criteria and Guidelines" document, prepared by the Safety Manager, enabled all design personnel to contribute safety assurance features throughout the design effort.

[illegible]

[illegible]

Fire Prevention

The approach to fire prevention was to minimize the use of combustible material and separate them from ignition sources. The major source of combustible materials in the vehicle is the engine fuel, type JP-5. Fire hazards in the use of this fuel are present during fueling and normal engine running.

Pressure fueling or defueling of the three tanks will be done only when the vehicle and fuel delivery system are properly grounded. The tanks are grounded through the vehicle structure. Prior to connecting the fuel delivery hose, a bonding cable is connected to both fueling truck and TACRV. Hence, the possibility of spark ignition, caused by the difference in static electricity potential, between the two vehicles, is eliminated. The possibility of fire in the compartments during [illegible]

[illegible] engine fire zones.

The fuel storage consists of [illegible] cells that are [illegible] the functional fuel tank [illegible] the personnel compartment [illegible] with polyurethane reticulated [illegible] explosion and flame suppression. [illegible] highly impact resistant, self-sealing [illegible] coupled with breakaway [illegible] valves. Each cell has [illegible] port connections at the top of the [illegible] to preclude crash rupture and fuel spillage. Ventilation and drainage is provided in the compartments where fuel system components and lines are installed.

The selection of non-metallic materials has been made with combustibility as a prime factor. In general, FAA-approved materials have been used wherever applicable. Non-flammable material is used in the cabin for rugs, seat upholstery, thermal and acoustic insulation and wall liner.

Fire Detection

The two general areas where a fire is most apt to occur are in the engine nacelles and in the PCU compartment. Since a fire in either of

these areas would greatly endanger both crew and equipment, a fire detection system is located in each of the engine nacelles and in the PCU compartment.

The means for fire detection is an element which changes resistance with temperature. This element is a continuous cable which threads through each engine nacelle so that it will detect hot spots or high average temperature. The detection circuit is triggered when a temperature of 450°F is detected. When this occurs the Master Caution Lights flash, an audible alarm sounds and the appropriate warning light goes on. The fire detection circuits have a "press to test" feature which allows the operator to test the continuity of the sensing elements and output amplifier.

Fire Suppression

The means for fire suppression is through the release of bromotrifluoromethane (CF_3Br). This material is stored in bottles, in a liquid state, and when released forms a heavy blanket of inert gas which excludes oxygen from the fire zone. This gas is released into the nacelles by the operator who presses a switch which ignites a pyrotechnic valve. Once opened, this valve allows all of the gas to be expended. The pyrotechnic valve switch is located so that the operator's Fire Control "T" handle must be pulled out first. This assures the cut-off of fuel and hydraulic oil flow to the engine compartments before the fire suppressant gas is released.

Fire suppression in the LIM PCU equipment compartment will also utilize CF_3Br. Detection of a PCU fire will be displayed on the Operator's Caution and Warning Panel and will also initiate the Master Caution Lights and Audible Alarm.

NORMAL AND EMERGENCY BRAKING SYSTEMS

LIM Braking

The Linear Induction Motors (LIMs) are capable of exerting the highest braking force of all braking modes provided for the TACRV and will be the primary means of stopping. However, LIM braking is dependent upon picking up wayside power, and the proper functioning of PCU equipment and controls. Hence, loss of wayside power, or electrical failures aboard the vehicles, will render LIM braking completely ineffective. The Braking System has been designed to have multiple devices for supplying braking forces. This permits evaluation of braking effectiveness, and enhances the safety of the crew and equipment during testing. High speed testing on a relatively short length of guideway requires back-up braking modes. With exception of the friction brake pedal, all braking device controls are within reach of both operator and observer.

Friction Braking

Friction braking has several important advantages over LIM braking. It is not dependent on wayside power and it is less complex; thus, the probability of failure is reduced. The friction braking system is also equipped with redundant actuators. The main actuators get high pressure oil flow from the three engine-driven pumps. Friction braking is the main back-up for LIM braking at low speed, whereas the speed brake is used at high speed.

Speed Brake

An aerodynamic speed brake, located on top of the engine nacelles, produces a drag force that augments vehicle drag for normal braking.

Emergency Braking Modes

As a backup to normal braking modes previously described, there are a number of emergency modes which assure stopping when primary braking fails. The friction brake pads have redundant actuators which are deployed by flowing hydraulic fluid from a charged accumulator. Thus, loss of pressure in the main hydraulic system will not void the use of friction brakes. A drag chute is aboard for use in major emergencies where falure or late application of a primary mode require additional braking force. Release of the chute is manual, through a cable-pulled mechanical latch; reliability is thus enhanced due to the direct, positive control. Friction braking can also be accomplished by shutting off the three engines, which causes the levitation cushion skids to rub against the guideway. If all methods of braking fail to stop the vehicle before it reaches the end of the guideway, an arresting cable engages

the nose of the chassis. As the cable extends, energy is expended in a water brake at the side of the guideway.

ELECTRICAL HAZARD PROTECTION

The vehicle and associated electrical equipments have been designed to provide ground paths so that protection of operating and maintenance personnel is assured. Electrical equipment in the vehicle body is positively grounded with straps or with aircraft-type approved bonding. Body-to-chassis grounding is done with grounding straps near the fore and aft suspension points. The LIMs are grounded to the chassis structure and to the LIM rail when the vehicle is not under way. The vehicle will be grounded during fueling.

VEHICLE GUIDEWAY RETENTION

The vehicle levitation cushions are designed so that the top of the cushion structure will engage the guideway guidance panels if the chassis lifts.

SUSPENSION SYSTEM

The suspension system is designed so that loss of electric power to the Control Amplifier Unit will result in the reversion from active to passive suspension. Other failures, which may affect only one channel of the active suspension system, will not cause automatic switching to passive suspension. The operator can select, with a mode switch, "passive suspension". This switch puts all actuators in the passive mode, and assures a safe, well damped ride.

CAUTION AND WARNING SYSTEM

The TACRV has a caution and warning system which is similar to that used in commercial aircraft. Two master caution lights, located on top of the operator's control and display panels, flash in the event of a detected failure or unsafe condition. These master warning lights alert the operator and observer to visually scan the control panels for a lighted caution indicator which identifies the malfunction area. Fire warning is separate from the "Caution and Warning System". Individual fire alarm lights designate the compartment in which a fire is detected and a horn provides an audible alarm. The areas monitored are the PCU compartment and left, center and right engine compartments.

NORMAL AND EMERGENCY EXIT PROVISIONS

The personnel compartment has a total of six possible exits for its occupants. Doors are provided on each side of the vehicle for normal and emergency exit for all occupants. If the doors are inoperative, two escape hatches above the operator seats can provide a means of egress. The direct-vision windows, just aft of the windshield, are designed to slide back, also permitting egress as a last resort.

PERSONNEL COMPARTMENT AND CRASH SAFETY CONSIDERATIONS

The design of the personnel compartment employs features that are consistent with approved safety and human factors practices for commercial aircraft. The selection of aircraft-type seats, restraint harness, bird-proof windshield, and the arrangement of instrument panel, caution/warning panels and controls, all contribute to safe and efficient operation of the TACRV.

Seats and Restraint System

For maximum protection of occupants, approved-type aircraft seats are installed in the personnel compartment. Safety belts and shoulder restraint harnesses are installed on the seats for protection during emergency braking conditions. The standard aircraft restraining harness has a single-point release mechanism that is capable of instant release by the occupant or by rescue personnel. The shoulder harness is equipped with an inertia reel and cable mechanism which prevents forward pitching of the body during emergency braking. A ratchet mechanism, within the reel, restrains the shoulder in the last angular position of the body when a sudden stop occurs. This device reduces chance of crash-induced head injuries.

IV. SYSTEM SAFETY PROGRAM APPLICATIONS TO ADVANCED PUBLIC TRANSPORTATION SYSTEMS

- PROGRAM PARTICIPATION BY SYSTEM SAFETY
- SAFETY ANALYSES METHODOLOGY
- SAFETY REVIEWS

This part of the paper describes System Safety Engineering techniques and methodology that are applicable to advanced public transportation systems of the future, derived as a "spin-off technology" from aerospace programs. Although recent commercial and military aircraft designs have utilized the systems safety discipline, design of surface mass transportation systems and automobiles has not. The TACRV is pioneering in high speed - 300 MPH - surface transportation. This alone produces a whole new spectrum of hazard potentials requiring system safety analyses for the first time. Failure Effects Analysis, Hazard Mode Analysis and System Integration Safety Analyses are useful "spin-offs" from aerospace technology which are applicable here. There has never before been any requirements for such in-depth safety studies in surface transportation. Formal safety reviews can be anticipated to resolve or correct hazards identified in all systems within the vehicle, guideway and related power distribution systems.

The contents of this section are graphically illustrated in Figures 4, 5 and 6, to depict the elements of formal safety program planning based upon the approaches used on aerospace programs. Figure 4 presents the typical safety program milestones for a prime contractor's Program Plan. Figures 5 and 6 provide insight into system safety participation during the design, manufacture and testing phases of a typical transportation system.

Safety analyses methodology is illustrated in Figures 7, 8, 9 and 10, also included in this section. These charts indicate the aerospace "systems approach" for effective utilization and coordination of analytical efforts, that may be applied to future transportation systems.

Several representative "tracked air cushion vehicles" for future public transportation are described in Part V of this paper. The purpose is to enable the reader to visualize the innovative approach to vehicle design, wherein system safety applications are essential, in the interest of public safety.

Aspects on Safety Programs Planning, Participation and Analyses

Based upon the approach used in the aerospace industry, the planning guidelines for future safety plans will be derived from Government Standard MIL-STD-882 and from prior contractor's experience on similar programs. The formal safety programs which include the application of analytical techniques and scheduled safety reviews will identify and eliminate, or reduce potential hazards associated with operation and maintenance of the overall system. In many cases, the use of safety devices, emergency systems, warning devices, or procedural changes will be employed.

Subcontractors will be subject to specific design safety requirements in the appropriate specifications and contracts. As technical systems manager, the prime contractor monitors all safety efforts of each subcontractor, ensuring that these requirements are met. On major subsystems, subcontractors are required to submit safety plans describing in detail their system safety organization, scope and effort. These plans will be integrated with the prime contractor's plan to ensure a coordinated overall effort that will include the following activities:

- Develop a "System Safety Engineering Program Plan", (SSEP) and submit to the customer for mutual agreement on scope, schedule and cost
- Perform preliminary (gross) hazard studies and system analyses on the vehicle, subsystems, operator station configuration, wayside power and guideway

systems (reference Figures 4, 5 and 7)

- Perform failure mode analyses on major systems to ensure that system or equipment failures will not cause hazardous conditions (reference Figures 5, 8, 9 and 10)
- Provide guidance and support to design personnel through development of safety design criteria and check lists appropriate for each discipline
- Define both design and operating safety requirements for all normal and emergency systems operation (reference Figures 4, 5, 6, 7 and 10)
- Develop safety procedures for compliance by operating and maintenance personnel before and after each vehicle run, to reduce chance of accidents or injury (reference Figures 4, 5, 6 and 10)
- Perform safety reviews during acceptance testing to demonstrate that operating and emergency procedures are adequate (reference Figures 4, 5, 6 and 10)
- Participate in design reviews and conduct safety reviews (reference Figures 4, 5, 6, 7 and 9)
- Monitor all pre-production equipment and systems tests to identify unanticipated failures modes and make recommendations for corrective action (reference Figures 5, 6, 8 and 9)

During subsequent vehicle tests, all previous analyses will be reviewed to assess adequacy of emergency provisions, develop operating and maintenance procedures, and monitor final test and checkout operations (reference Figures 5, 6 and 8).

- SAFETY ANALYSES METHODOLOGY
  - OBJECTIVES:
    HAZARD IDENTIFICATION, ELIMINATION AND/OR COMPENSATING PROVISIONS
  - SAFETY ANALYSES UTILIZATION FLOW
  - PRIME AND SUBCONTRACTOR ANALYSES, A COORDINATED EFFORT
  - COORDINATION OF RELIABILITY "FMEA" WITH SYSTEM SAFETY "HMEA" ANALYSES

V. A LOOK AT FUTURE MASS TRANSIT SYSTEMS

- ADVANCED CONCEPT STUDIES
- SYSTEM SAFETY OBJECTIVES

ADVANCED CONCEPT STUDIES

The growing need to improve our nation's surface transportation systems is currently recognized. While improvement of existing modes is a logical step, we are also pursuing new and innovative concepts as the only means through which a dramatic upgrading of ground transport can be achieved. The tracked air cushion vehicle with linear induction propulsion is an excellent example of a developed concept that employs technology new to the transportation field. TACV promises a safe, fast, comfortable, all-weather, non-polluting alternative to present systems. Applications of this concept, in the near future, will provide a major first step toward gaining public acceptance of this new mode of travel. The TACV is considered to be an innovative approach to provide high-speed ground access to our airports, as well as a safe and comfortable means of inter-city mass transit, for the near future. Figures 11 and 12 illustrate typical development studies of the aforementioned Tracked Air Cushion Vehicles.

SYSTEM SAFETY OBJECTIVES

The system safety objectives that are considered uppermost in the TACV System and all new modes of transport development, are as follows:

- The system must ensure safety of passengers, operators and maintenance personnel
- The system should not create or appear to create a hazard to the community, its environment, its children, or its animals
- The operational reliability must be sufficiently high and recovery from failures that do occur must not present a potentially hazardous condition to people, equipment or other means of transport close proximity to the system
- The system should not pollute the operating environment with exhaust or excessive noise

In summary, the primary objectives of the System Safety Engineering Programs planned for new modes of public transportation, include the following:

- Identify potential hazards by analytical methods and by equipment test surveillance
- Determine hazards effects on passenger and public safety
- Develop corrective and/or preventative measures
- Identify rescue requirements peculiar to new transportation system
- Establish safety guidelines for design, test operation and maintenance phases of vehicle life cycle
- Identify need for technology development and additional study where safety assurance appears uncertain

VI. SUMMARY AND CONCLUSIONS

SUMMARY

The concept of System Safety Engineering has matured with aerospace programs and is now contributing safety assurance methodology to the non-aerospace segments of our society. As an appropriate example, a Safety Engineering effort discussed in this paper, has been "tailored" to the particular design, schedule and operating requirements of the Tracked Air Cushion Research Vehicle (TACRV). The safety considerations used during the design of TACRV are the result of experience gained from a wide range of aircraft, space vehicles and experimental systems designed and manufactured by the Grumman Aerospace Corporation. The incorporation of the appropriate features into the TACRV design provide the desired result of a safe research vehicle with minimum hazard to operating personnel.

In many cases, materials and hazard control techniques developed in our aerospace programs are being applied to advanced surface transportation systems. Typical examples in TACRV are use of non-flammable materials, system hazard and human factors studies, redundant systems for critical control functions, and fire-proofing of fuel and propulsion systems.

It is anticipated that many of the approaches to safety assurance described in this paper will be directly applicable to future public transportation systems and vehicles as a "spin-off technology" from the aerospace industry.

In summary, the significant safety features provided to compensate for potential hazards identified on the aforementioned TACRV, include the following:

POTENTIAL HAZARD CATEGORY	COMPENSATING SAFETY PROVISIONS
Fire and Toxic Smoke	• ECS Fresh Air Supply System, Two Sliding Windows, Two Overhead Hatches • Fire Detection and Suppression System for Critical Areas • Non-Flammable Materials in Personnel Compartment • Fire Shut-Off Valves for Fluids
Explosion	• Crashworthy Fuel Tank and Lines; Fuel Tanks Assembled with Reticulated (Porous) "Safety Foam" • Fuel Tanks Isolated From Crew • Drainage and Ventilation in Fuel Area
Emergency Stopping and Crash Condition Hazards	• Aircraft Seats, Safety Belts, Shoulder Harnesses and Inertia Reels • Padded Instrument Panel Visor • Two Doors and Two Escape Hatches

POTENTIAL HAZARD CATEGORY	COMPENSATING SAFETY PROVISIONS
Brake Failure Emergencies	• Friction Brake Backup System • Drag Parachute • Arrestment Cable System • Settle Vehicle on Cushion Skids
Critical Systems Failures (i.e., Fluid Power, Electrical, Turbofan [illegible]ines, etc.)	• Caution and Warning System Located on Operator's Panel
Electrical Shock to Personnel	• Vehicle Grounds Externally to LIM Rail When Vehicle Stops, Plus External Grounding Cable Provided • [illegible]ernal Vehicle Bonding and Grounding [illegible]ents
Bird Strike Hazards to Crew	• Birdproof Aircraft Wind[illegible]
Fog, Rain or Ice on Windshield	• Electrically Heated Aircraft Windshield
Secondary Suspension System Malfunction	• Operator can Switch From Active to Passive Suspension System
Vehicle Leaves Guideway	• Positive Retention of Vehicle Provided by Air Cushions Extended Under Guideway Side Rails

CONCLUSIONS

Judicious use of System Safety Engineering techniques during early phases of design can yield a highly effective safety assurance program in terms of accident prevention, avoidance of costly changes and assurance of safe operation and maintenance, throughout the life cycle of the system.

Timeliness of Safety Engineering studies is an essential factor for early identification and elimination of potential hazards and latent design deficiencies. By this approach, the appropriate safety devices, emergency systems and fail-safe features can be readily incorporated during the initial design stages.

The Grumman approach to system safety is "the total integration of available skills and resources to achieve maximum safety assurance". Safety program activities generated by this "system approach" and total team effort yield an effective program without costly duplication of efforts.

As we pioneer into higher speed concepts of surface transportation, extensive application of in-depth failure and hazard mode analyses, systems integration analyses and formal safety reviews can be anticipated, in the interest of passenger and community safety.

VII. REFERENCES

1. Military Standard MIL-STD-882; "System Safety Engineering Program for Systems and Associated Subsystems and Equipment; Requirements for."

2. "AFSC DH 1-6 System Safety Design Handbook": Published by USAF Hdq. Air Force Systems Command; Wright Patterson AFB, Ohio 45433.

3. HARRY E. Arnzen, "Implementation of Prime and Subcontractor System Safety Engineering Programs"; Grumman Aerospace Corporation, Bethpage, New York, June 12, 1970.

4. "System Safety in Transportation"; System Safety Society, Washington, D.C. Chapter Newsletter, 18 March 1971.

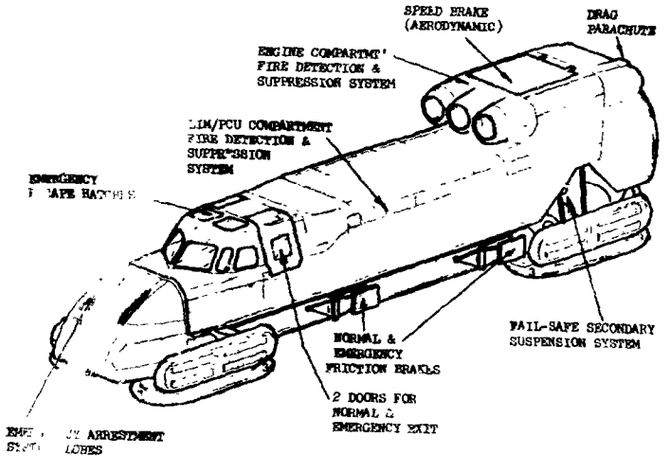
5. "System Safety Engineering"; Approach Magazine, Pages 38-42; Published by Navy Safety Center, Norfolk, Va., March 1970.

6. Harry E. Arnzen, "Failure Mode and Effect Analysis: A Powerful Engineering Tool for Component and System Optimization"; - 5th Reliability & Maintainability Conference; Annals; AIAA/SAE/ASME; New York, July 18, 1966.

7. "Proceedings of USAF - Industry System Safety Conference, Las Vegas, Nevada"; Published by Directorate of Aerospace Safety, Norton AFB, California; 25-28 February 1969.

8. Roy Harris, "Preliminary Hazard Analysis", TRW Systems Corp., Redonda Beach, California; Proceedings of USAF - Industry System Safety Conference, Las Vegas, 25 February 1969.

9. The Boeing Company, "Fault Tree for Safety", DG-53604, November 1968.



TRACKED AIR CUSHION RESEARCH VEHICLE SAFETY PROVISIONS

FIGURE 3

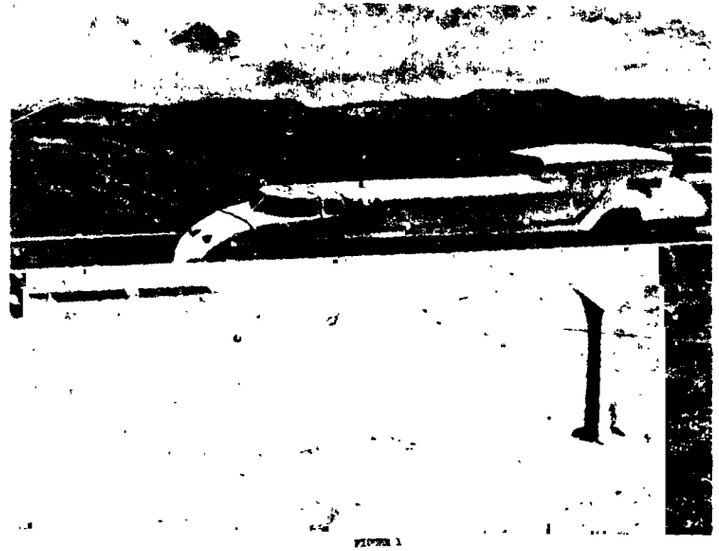
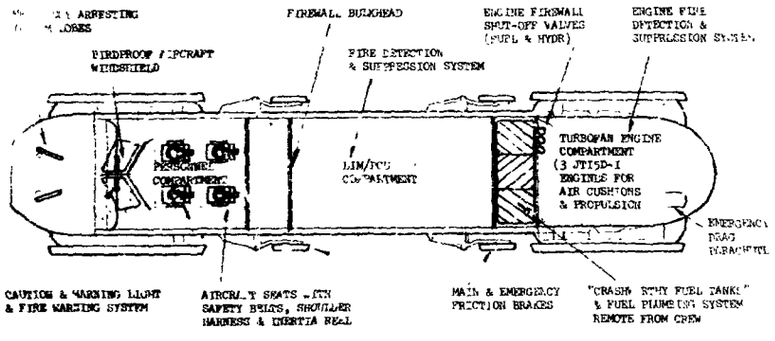


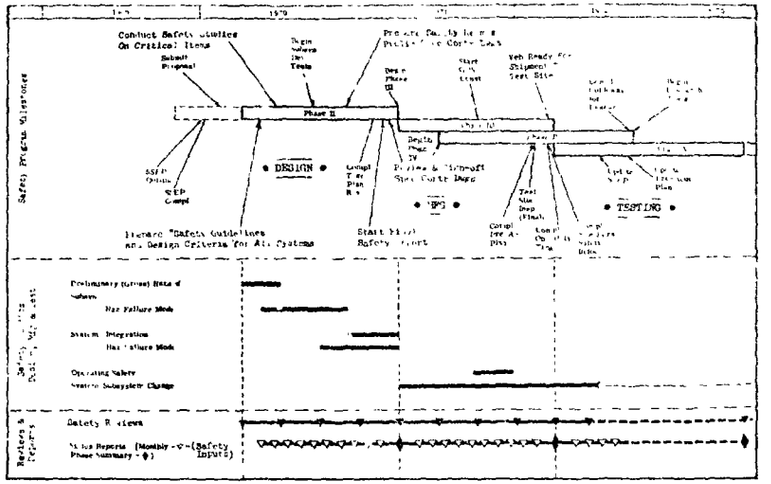
FIGURE 1



TOP VIEW

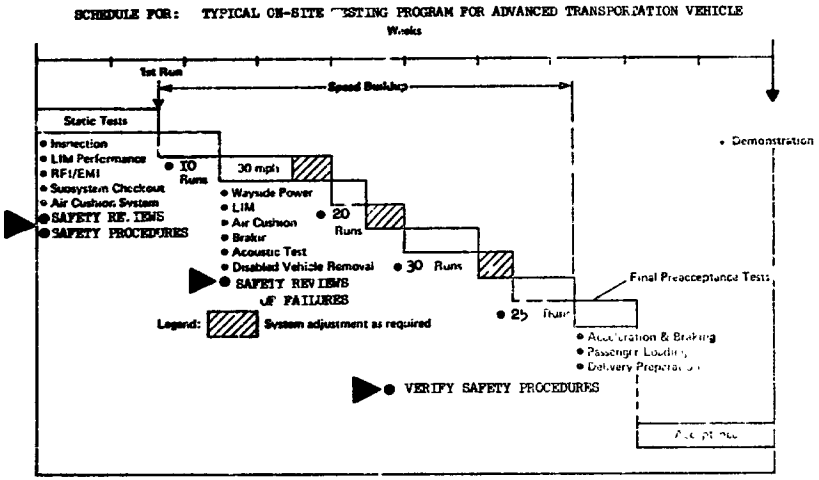
● TRACKED AIR CUSHION RESEARCH VEHICLE SAFETY PROVISIONS

FIGURE 4



SYSTEM SAFETY ENGINEERING PROGRAM MILESTONES FOR TACV

FIGURE 2



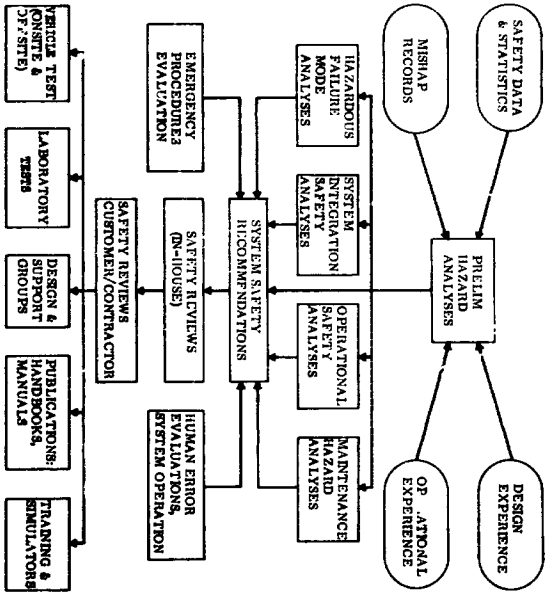
● SYSTEM SAFETY ENGINEERING PARTICIPATION IN TEST PROGRAM

FIGURE 7

SAFETY PROGRAM TASKS	6 MONTHS	12 MONTHS	18 MONTHS
1. APPROVAL OF "PROGRAM PLAN" (SSEP)	▲		
2. PRELIM HAZARD ANALYSIS	▲ START ▲ UPDATE	▲ UPDATE	▲ COMPLETE
3. SYSTEM SAFETY ANALYSIS	▲ START	▲ UPDATE	▲ COMPLETE
4. SUBSYSTEM SAFETY ANALYSIS	▲ START	▲ UPDATE	▲ COMPLETE
5. INFORMAL SAFETY REVIEWS ("IN-HOUSE")	▲ PERIODICALLY - EACH SUBSYSTEM & SYSTEM		▲
6. FORMAL SAFETY REVIEWS (CUSTOMER/CONTRACTOR)	▲ QUARTERLY	▲ QUARTERLY	▲ QUARTERLY
7. MONITOR ALL "IN-HOUSE" TESTS	▲ AS TESTS ARE CONDUCTED		▲
8. MONITOR SUBCONTRACTOR SYSTEM SAFETY PROGRAMS	▲ START/THROUGHOUT PROGRAM		
9. MONITOR VEHICLE TEST PROGRAMS/ONSITE & OFFSITE	▲ START/THROUGHOUT PROGRAM		
10. PREPARE SAFETY "CAUTION/WARNING" PUBLICATIONS FOR OPERATORS, CREW, MAINTENANCE & TESTS PROCEDURES		▲ START	COMPLETE ▲

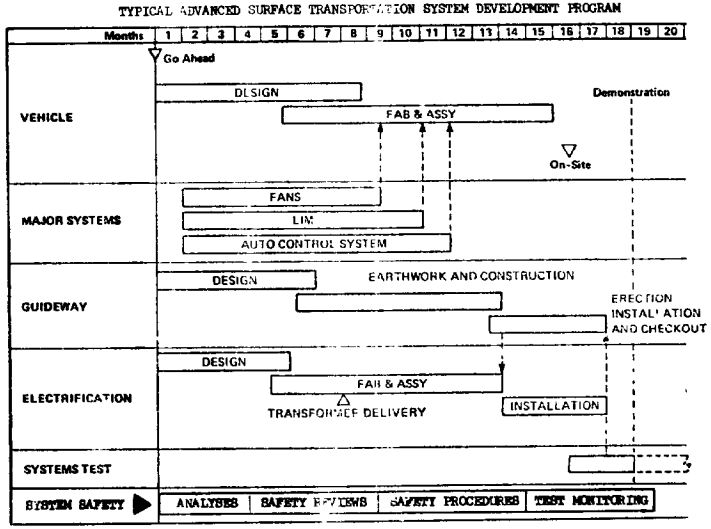
● TYPICAL SAFETY PROGRAM MILESTONES FOR A PRIME CONTRACTOR BASED ON AEROSPACE PROGRAM PLANNING GUIDELINES

FIGURE 5



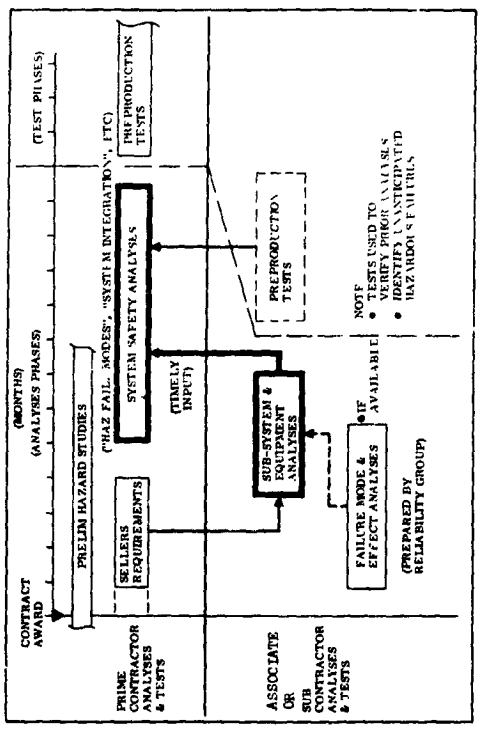
● SYSTEM SAFETY ANALYSES UTILIZATION FLOW CHART

FIGURE 8



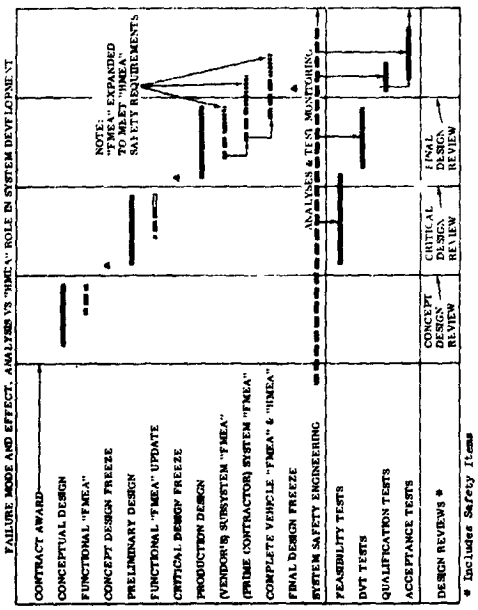
● SYSTEM SAFETY PARTICIPATION DURING DESIGN AND MANUFACTURING

FIGURE 6



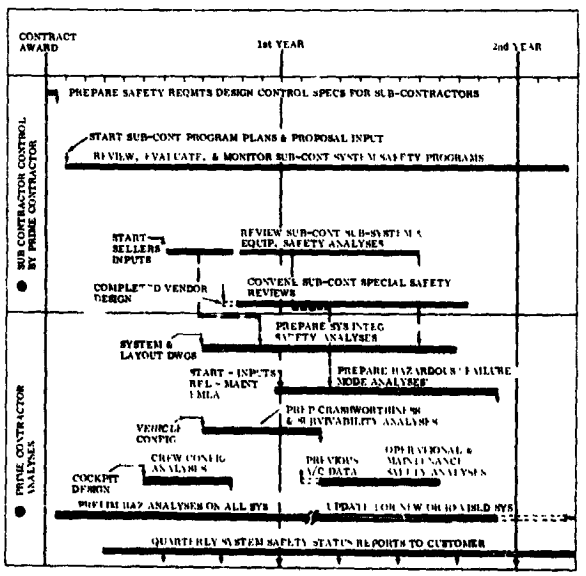
● USE OF PRIME AND SUBCONTRACTOR ANALYSES AND TESTS AS A COORDINATED EFFORT

FIGURE 9



● PREPARATION OF "FAILURE MODE AND EFFECT ANALYSES" AND "HAZARD MODE ANALYSES" AS A COORDINATED RELIABILITY/SAFETY EFFORT

FIGURE 10



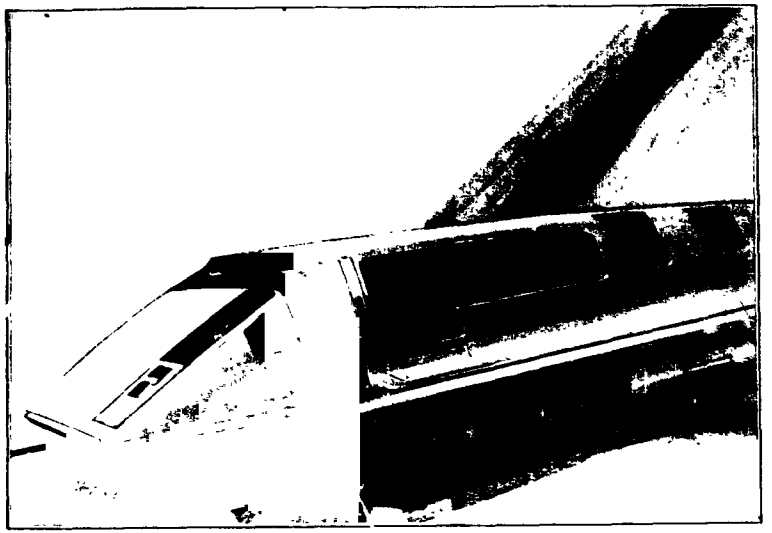
● TYPICAL AEROSPACE PROGRAM PLANNING CHART FOR COORDINATING PRIME AND SUBCONTRACTOR ANALYTICAL TASKS

●● SERVES AS A GUIDE FOR PLANNING NON-AEROSPACE SYSTEM SAFETY PROGRAMS

FIGURE 11

LOCKHEED-GEORGIA CO., VIBRATION OF JACT

FIGURE 12



LOWEY-SMAITH INC. VISUALIZATION OF TACV

FIGURE 13

SESSION VI

QUESTIONS AND ANSWERS

JERRY LEDERER: Mr. Arnzen: If you have those two high speed tracked vehicles going to opposite directions and apparently very close together according to the slide, what do you do about the negative pressure between the two vehicles, aren't they going to be drawn together? Question No. 2 - The Airlines have for years used JP-4 for safety What do you use JP for? No. 3 - In connection with the bird strike on the windshield, are you considering the possibility of things like icicles hanging down from bridges hitting the windshield too. They can be pretty tough.

MR. ARNZEN: In regard to the first question, this is a necessary portion of wind tunnel research. I believe you struck on a very good point: the bow wave from one vehicle would impart a shock wave against the opposing vehicle coming in the opposite direction. I believe this would be an essential part of the wind tunnel work to study this interaction. Conceivably it could be a violent whack and you might call it similar to two snow plows passing each other with a three-foot gap. The wind tunnel data would indicate the optimum distance. Conceivably, it might be better to put one guideway on one side of a turnpike, whether it be an interstate parkway or priority real estate already assigned, and perhaps the wind tunnel data would tell us it should go on the opposite sides. In regard to the use of the fuel. These particular engines, the engine manufacturer recommended use of this, this is not our selection although one fuel would be slightly less volutable than the other, we think we have eliminated the volutable problem by the non-destructive crashworthy tanks, the well-ventilated compartments of these tanks, the isolation from vapor even getting into lem compartment and the overboard venting procedures during refill. We are aware of many precautions which have to be taken in handling this fuel. The last question in regard to bird strike damage, on Gulfstream 1 and 2 we have conducted tests with 15 lb. birds and this is interesting. You actually can encounter certain birds up as high as 30,000 feet. Destructional integrity is such of these crash resistent windshields that they will take bird strikes. However, the gentlemen who referred to the transit program and the various problems presented came up with something interesting which we have to put in our cap. Bricks dropped by children from overpasses, icicles and things of that sort, warrant new and fresh consideration. There will be a whole new spectrum of hazards--a whole new ball game and I think that is a good question.

QUESTION: Mr. Driver, everyone has a car so everybody is an expert. Assuming that speed of course is by definition a problem on the road, in the diagrams that you showed I saw nothing being done about what might be described as too much engine and not enough bumper. Is anything being done in that area or contemplated?

MR. DRIVER: We have out now a notice that controls rulemaking which addresses the problem of speed control. It identifies speed warning and speed control, they are two separate functions. One to advise the driver that he is going too fast and the other one is to keep his car from going too fast, either by virtue of control of horsepower or by virtue of a speed control device like a governor. In the area of bumpers, amazingly enough most of the bumpers that you now have will not survive a two-mile an hour impact, without humping the front end. I have had personal evidence and I guess most of you have had also. We are now proposing a five and a ten mile an hour bumper however the bumper is just the first thing to get hit and is just a part of the total energy absorption system that we are trying to develop for a vehicle. This will include not only "energy absorbing bumpers" but also "energy absorbing front ends." For example, the hinge front end, Ford now calls it the X-member. Shock continuation through the entire body frame plus

the passive restraint to keep you where you should be so you can ride down the G forces instead of smacking up against the interior of the vehicle at High-G forces. We think we are taking a systems look at it. Those two you mentioned are a part of the total problem.

R.M. WILMOTTE: This is really a comment about a statement of Mr. Williams. The comment I want to make is in connection with operating correctly the first time. I think there is a danger in referring to doing anything correctly. There is always a residual failure, a residual uncertainty and that comment has influences if you say that you have done something correctly the first time. It influences two groups; one management, the manager says well now I can do what I want I have no dangers, but there is always a probability of a danger. The second is the operating level I'll give you the example of the well documented zero defect propaganda. I'll quote a comment from a manufacturing engineer manager whom I held very highly. His statement was something like this; After the President had made his one-half hour speech saying we must have zero defect in this company etc., there was an improvement in his shop for something like two weeks and then it fell back, not to where it was, but something to worse than it was. What were reasons? The reasons are rather interesting. He said, before that speech I used to know pretty well where in my shop the troubles came, and I was generally told about them in some way or other. After that speech there was a very wonderful cooperation among the workers that they wouldn't tell me where the troubles were and I couldn't find them anymore. From that point of view the product of my shop dropped. I heard that specifically from this individual but I also heard a confirmation of that in other places so I would like to give a warning, the possibility of using in any form, that anything can be perfect or that anything can be done right the first time has associated with it certain dangers.

The next thing that I want to say concerns Mr. Driver. I am always interested in the relationship between an activity that looks as though it was self-contained but never is. It is always connected with some other activity. You've been concentrating, and I'm sure you know what I say is quite obvious to you and you know it thoroughly, but your description refers entirely to the saving, the safety of life, I'll say or reduction of accidents. You cannot isolate that from the cost. Politically we say to save a life is worth an infinite amount of money, well, that just isn't true because we never do that. In the case of automobiles you have two ways of obtaining a price for safety. One is by taxing in which the federal government or the state governments impose a regulation, impose a tax and pay for some things such as improving the road bed. The other is to impose a structure in the equipment which costs something and is politically easier to handle because it merely is represented in a price which the buyer doesn't know specifically how much of that is for safety and how much is for better paint or something. Besides the price angle, there is the pollution angle. Does the safety requirement that you put on increase pollution? I suggest that generally it does. The real problem, I give you an example that came rather interestingly; There were a number of accidents on tractors and the tractor manufacturer improved his tractor in order to reduce the accidents and indeed it was a pretty good improvement but strangely enough the number of accidents remained the same. Why? Because the operators of the tractors now used it in more dangerous conditions because there were less accidents. Until the number of accidents drew up to about the same as they were before then they stopped endangering the equipment. There is a strong tendency which I think is very much to the point of the automobile process. You will find over the years that the accident rate strangely enough has remained remarkably constant with all kinds of changes that have been put in. It is true that recently there has been a decrease. But there were decreases like that as something happened and for a while it decreased; but there is a tendency to go back. In other words, I think that probably we are generally increasing the speed of our automobiles up to the point that we don't like to get killed anymore. That is, we hear of our friends or people know of someone who has been killed in an automobile accident. If we hear too

much of that then we drive more carefully. If we hear less of that we drive less carefully. We speed up and there is a tendency to, I think you'll find some literature on the subject, for humans to build up their danger up to a certain point and strangely enough that point is very much the same in all kinds of accidents. In the case of automobiles and where we put heavier bumpers and reduce the accident rate because of something of this kind, you are likely to find over the years, if the philosophy I am describing is correct, you will describe over the years, first of all a increare in weight of automobiles which will use more gasoline for more pollution. Secondly, a higher speed because there are few accidents, therefore, we want to build up the accidents and one of the benefits of course of all this is that you want to balance not only the accident rate but the price. The pollution and the value of the automobile. Namely reducing time and under the strange pressure that our society and civilization has built, time seems to be not necessarily measured in dollars but I don't have time to do what I want to do therefore I want to go fast.

MR. DRIVER: I'll respond yes. No. 1 on cost to save. I quite agree that there is a cost penalty for practically any innovation or anything new. In our case what we try to do is to institute a performance of clamor with such an effective lead time that it can involve only redesign of an existing piece of equipment. Like redesign of a brake instead of add on of another piece of equipment. This cuts the cost down quite a bit. In addition, some of our performance requirements involve the elimination of some parts of the vehicle and the substitution, say the elimination of two pieces of equipment and the addition of one piece of equipment so that in many cases the cost is balanced off. We do run safety cost benefit analysis in each case to determine and we hate to equate the life to a dollar but you have to do it sometime and we take a good hard look at what are we getting for our money. If we institute safety device or safety requirement No. 1, approximately how many lives are we going to save, how many injuries are we going to reduce. How many crashes are we going to avoid? We equate that with how much it is going to cost you as a consumer per vehicle to get that. Then we take a look at those figures. If they are in the red it doesn't mean we won't do it. I'll give you a very concrete example. The furor about power windows. A safety standard came out on power windows, it required certain minor changes to the power window system, in actuallity the number of lives lost as a result of improper action of power windows was low but those that happened to get killed happened to be kids and one of them happened to belong to somebody in pretty high places. The same thing of school bus standards, you have many more school kids getting killed in automobiles than you have getting killed in school buses but what do we do for automobiles to protect children, what do you do for a school bus when something happens. In summary, we are doing something and we are trying to implement it in such a way that the cost is minimized. In terms of increase in pollution, the only standard that I know of that pertains to pollution in our particular case is one that reduces it and that is the one on the fuel tank for example. The fuel tank is no longer vented to the atmosphere and if I remember my figures right from when I was working on the low pollution automobile about 15% of your vehicle pollution is plain ole evaporation out of the fuel tank. I admit that if we would come out and require that vehicles have bigger engines and lower rpm etc. and give more exhaust out of the exhaust you might be adding to pollution, I'll just quarrel with you on that a little bit that's all.

N72-25988

OBSERVATIONS AND REFLECTIONS

by

Jerome Lederer
NASA Director of Safety
NASA Headquarters

Presented at the

System Safety Conference, GSFC

May 26, 1971

This has been a very stimulating meeting. Before making my observations and reflections I feel we should thank Phil Bolger for organizing it.

I'll begin with a few criticisms.

The emphasis was on hardware, yet software is of vital importance. Miller and Arnzan tried to drive home the fact that system safety covered more than engineering. Mistakes in procedures, in computation, even the way words are used in a manual are important. They may be misinterpreted or misunderstood. My boss in the Office of Manned Space Flight, Dr. George Mueller, had a large and unusual photograph on the wall behind his desk. Figure 1.

It was simply a photograph of a minus (-) sign. Some years ago a computer programmer had neglected to feed the minus sign into an equation going into a computer to guide a space vehicle. This "software" mistake cost about $18 million, as I recall. So do not forget software when you think of system safety.

Other important subjects, not hardware oriented, are part of System Safety or the systematic approach to loss prevention. Some 30% of missile failures have been caused by human errors. Yet in these lectures there was little or no reference to motivation and certification programs. Motivation (awareness) is an important part of the NASA program. The blue collar worker can be the Achilles heel of programs that depend on single point failures. The only reference to motivation was the NASA Awareness Bulletin on the table. Mr. Pope alluded to motivation when he stressed the importance of communicating up. I heard very little about human factors. Gera of NAR did have behavior failures in his closed loop vugraph. Human factors should be considered to include the environment in which men work, the shop, test center or the cockpit, as well as human factors in the design of the product such as shape of control handles.

Except for the lecture on Viking, I heard no reference to Safety Analysis Reports. This is a vital report prepared for the top decision maker prior to operation, showing him what risks remain, how they are rationalized, why they were accepted. Without this, top management cannot give or deny a go-ahead, with prudence.

Another criticism is the problem to which C. O. Miller alluded, of making writing easier to grasp. Much of our phraseology is hard to understand by managers whom we are trying to influence. Pope suggested a replacement phraseology such as "performance error" in place of the word "accident" in order to make safety (a motherhood term) more acceptable in management circles. His recommendation to change an accident report into a management critique written by the people involved in the accident is another excellent idea in my opinion. He questions the use of the word Safety. I'm sure he has wide support. We prefer risk management. What is meant by "critical" in the phrase "critical hazard analysis." Why not simply use hazard analysis. "Optimization" is frequently used. What does it mean? Why use cycle in "life cycle?" I suggest that the phraseology of system safety be combed for simplification. It is also of great importance to do this when system safety is translated from aerospace to other industries. The lecture by Williams brought this out.

There is background to use palatable words in aviation safety; lap belts or seat belts in place of safety belts is an example.

The first group of papers was devoted to the philosophical aspects of system safety especially the management aspects. Dr. John Clarke, Congressman Pettis, Admiral Smith discussed the nature of the problems that face us. Dr. Wilmotte lectured on basic personal resistences to the acceptance of safety. Later on, Hurt of USC on System Safety Education added to this. It is not unusual for sophisticated management and non-safety personnel to feel that safety acts as an obstruction to progress. Could these resistences, voltages, amperages be put into the form of a model electrical circuit for further analysis?

Dr. John Clark pointed out that if safety were applied to unmanned vehicles as it is applied to manned vehicles, it could cost the unmanned vehicle out of existence. This is also true of manned vehicles such as aircraft. Space vehicles are a special problem because of the serious political and prestige implications of mission failure. This justified the $100 million dollars or so spent to correct the faults shown up by the 204 fire. In the case of more mundane vehicles there comes a point where small increments of increased

safety are hard to justify on the basis of cost benefits. For example, Slides 2, 3.

An example of cost benefit is the current requirement for crash fire rescue operations at airline airports. Relatively few airports meet the minimum requirements of the National Fire Protection Association. Most airline crashes occur on the approach to a landing off the airport where the crash fire equipment cannot get to the crash quickly. A ten year survey made for the piston era disclosed only two crashes in which a fire brigade saved the lives of airline passengers. To meet NFPA requirements would have added some $80 million per year in firemen salaries alone, with the possible saving of 10 lives per year. These lives of course should be saved. The airlines would have to pay for this via landing fees. But resources are limited. Passenger safety would be better advanced by applying this sum to the implementation of landing aids such as ILS and approach lights and other means by design or procedures to prevent the accident. Now with funds from fuel taxes to be applied to the development of airports and airways, progress should be better. Is it easier now to justify $80 million or more for crash fire protection because aircraft are carrying more passengers, more cargo and the structures on the airport are costly enough to support the expenditure for adequate fire fighting brigades.

The cut off of money for safety is a management decision, as Gera said. The safety organization should provide the basis for this judgment. It should not be left to the staff that creates the problems or are willing to accept the hazards or fail to recognize them.

Styles' paper on the Application of System Safety to Rail Transit Systems inferred this and gave proof of the need for a monitoring program. His paper supports Dr. Wilmotte's paper describing how and why management tends to underestimate risk.

During the course of this conference there was a question or two about measuring the economics of safety. This should be done by searching for the total economic impact of accidents on society. For example, the number of passengers killed by railroads is very small, but in their total operations, the railroads in 1970 killed more people than the airlines and general aviation combined (largely because of the grade crossings). The impact of accidents on society might be measured by the loss of the deceased's useful service to society. The following slides bring this out - slides 4-10.

Congressman Jerry Pettis's inspirational talk urged the application of space age techniques, especially the systems approach to solve our many problems on earth. The agenda was slanted that way in relation to hardware, not social problems. We had talks on application of system safety to nuclear safety, consumer product safety, rail transit safety, auto safety, petroleum safety, and advanced surface transport safety. These are not the social ills which Mr. Pettis wants attacked. On the same morning that Congressman Pettis gave his talk the New York Times reported this -

> "If we can go to the moon, it is often said, why can't we solve some of our pressing problems on earth? Speakers at the Urban Technology Conference here stressed the point yesterday that solutions on earth were not as neat and straightforward as developing a space-flight system."
>
> "Aerospace technologists were told yesterday that they must come out of the clouds and understand political considerations, city finances, labor problems and human relations before they can help the nation's cities solve their transportation needs. There is much more than technology to solving these problems, James M. Beggs, Under Secretary of Transportation, told aerospace industry representatives at the Urban Technology Conference at the New York Coliseum.
>
> When I was asked to come to the department, he continued, I was asked that old saw: 'If we can go to the moon, why can't we get across town?' Well, the reason, I learned, is that it's tougher. There are people in the way of getting across town, and there aren't any people on the way to the moon."

One reason for the success of space age performance or for that matter most successes in business is that a dictatorship or an autocracy exists which gives orders with

considerable assurance of compliance. Not so with social problems, at least in a democratic society, until a crisis occurs. The crisis of pollution is beginning to draw people together socially to fight that problem. People tend to protect their individual prerogatives, using the democratic system to do so.

I'm afraid that Mr. Beggs is correct. The enemy of people are people. Is there a system technique to tackle this?

In my opening comments I referred to lawsuits based on product liability as a forcing function to stimulate adoption of system safety. I was interested therefore in Mr. Hayes comment that "a prudent and reasonable person would make a system analysis to avoid being held guilty of negligence in lawsuits."

Styles (and others) pointed to the well known feeling among design engineers that they do not need the help of safety specialists because they know all about it. Then he proceeded to give a devastating attack on this belief in his account of errors made in rail transit design. Dr. Ball indicated that the DOD was considering a process of deemphasizing system safety as an independent discipline. But the weakness in the argument that the engineer/designer needs no independent risk management help is that -

He is subject to the dictates of his immediate supervisor who must contend with schedules, performance, costs, politics. In short, the engineer, in spit of his Canons of Ethics dealing with safety, is an organization man. He depends on his organization (boss) for a living.

He is not generally exposed to the safety interfaces, e.g., the design of railway car for safety is often not coordinated with the design of the station platforms for safety (except for height), as Styles pointed out.

While he considers himself an employed professional, and he is, this is not in the sense of the independent professional such as a Physician who can more easily abide by the Hypocratic Oath than the engineer can abide by the Canons of Ethics. This is because the physician is not an organization man and furthermore because he see. the end product of his labor--the patient who lives or dies. If engineers could see the injuries caused by their design they too might be more forceful in their safety work. Decision makers should be given the safety picture by an independent source, not by men subject to other pressures or who create the problems. Dr. Wilmotte emphasized this.

Suppose we were meeting here in 1889 instead of 1971 and our topic of discussion was "Should the Automobile Be Encouraged From the Standpoint of Safety?" What would our decision be if a systems analysis were to show that the automobile would kill a million people in 50 years, maim millions more, pollute the air. On the other hand the automobile would also save millions of lives, offer independent means to get out of the city, get to far off places unexpensively with one's family, improve the standard of living of millions. Could you come to a rational decision, balancing the good against the bad? Using what we know about system analysis now, most of the negative aspects of the automobile would probably have been engineered out.

These remarks are personal and do not represent the official opinions of NASA.

[redacted]

FIGURE 1

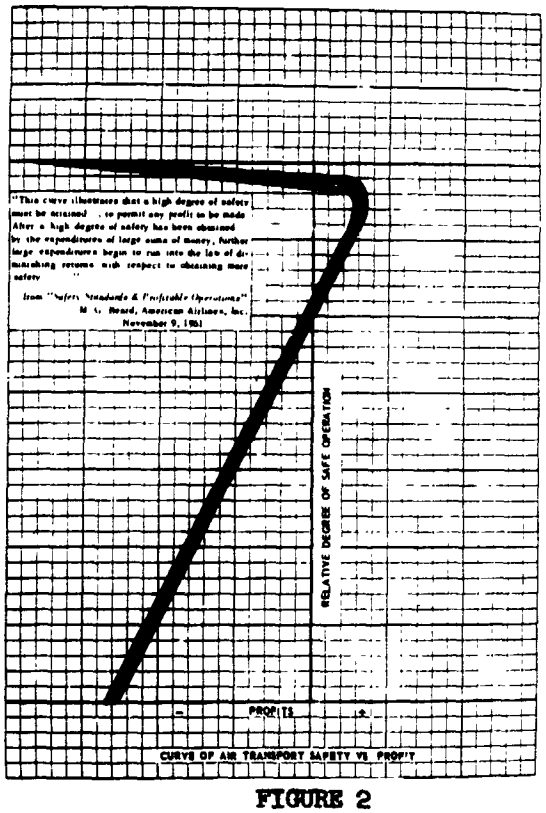
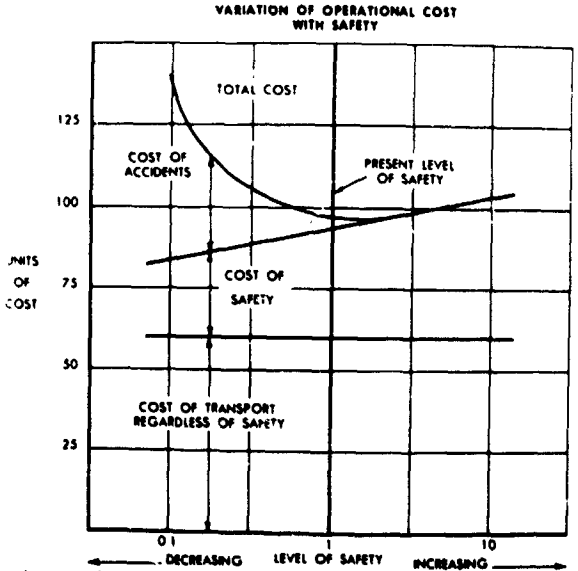


FIGURE 2



or the purpose of this chart, the total cost for operating aircraft consists of the basic cost of transport, lus the cost of safety, plus the cost of accidents. As shown to the left of the median line, a sub-tandard expenditure for safety will result in a high cost for accidents which, in turn, will result in ugher total operating costs. However, as expenditures for safety are increased, the cost for acci-lents will decrease until a point is reached where safety costs add to rather than decrease total operating costs. It is at this point (where, for example, the expenditure of $80 millions for crash-re rescue equipment may only save 10 lives annually) that the laws of economics raise policy questions of monumental difficulty for private operators and public authorities. Source: Walter Tye, ritish Air Registration Board, "Unresolved Civil Airworthiness Problems," Institute of the Aerospace ciences, Inc., 1959

FIGURE 3

FIGURE 9

FIGURE 10

☆U.S. GOVERNMENT PRINTING OFFICE: 1971-720-050/308